Chapter 5 Revision History as of November 30, 2021

- Revised Entire Document

This page intentionally blank

Chapter 5
Classified Matter Protection and Control

This chapter describes the security procedures adopted by Department of Energy (DOE) Headquarters (HQ) to implement the requirements of the following DOE directives:

- 32 Code of Federal Regulations (CFR) 2001 and 2003, *Implementing Directive*
- Atomic Energy Act of 1954, as amended
- Executive Order 13526, Classified National Security Information
- National Security Act of 1947, as amended
- Executive Order 12333, United States Intelligence Activities, as amended by Executive Order 13355
- DOE Order 471.6, Admin Chg 3 *Information Security*
- DOE Order 475.2B*, Identifying Classified Information*
- DOE Order 452.8, *Control of Nuclear Weapon Data*
- DOE CMPC Marking Resource
- CG-SS-5, Classification and Unclassified Controlled Nuclear Information Guide for Safeguards and Security Information

The common objective of these directives is to protect classified information from unauthorized disclosure to potential adversaries who may wish to attack U.S. security interests, harm the American people, or develop weapons of mass destruction.

- Section 501 describes the roles and responsibilities of HQ employees who have access to, possess, or generate classified information. It also outlines the roles and responsibilities of those involved in implementing the Classified Matter Protection and Control (CMPC) Program at HQ. Finally, it lists the various training requirements for personnel with Q and L security clearances and those performing specialized CMPC functions.
- Section 502 briefly describes the HQ classification program and the appointment of Classification Representatives.
- Section 503 describes the four categories and three levels of classified information in use throughout the U.S. Government, special designators unique to DOE, and other special handling controls.

- Section 504 describes the specialized topic of identifying and handling classified, or sensitive information generated by foreign governments.

- Section 505 describes the procedures for preparing and marking classified matter. The *DOE CMPC Marking Resource* is an invaluable tool for properly marking all types of classified matter.

- Section 506 describes how to protect classified matter while it is out of its normal storage container and in use.

- Section 507 describes the procedures and equipment required to properly store classified matter.

- Section 508 describes the procedures for reproducing classified matter and identifying the equipment that can be used.

- Section 509 defines what classified matter must be accounted for and the accountability mechanisms to be used by HQ elements.

- Section 510 discusses the requirement for each HQ element that receives, or dispatches classified matter to establish a Classified Document Control Station (CDCS) to centrally manage such transmittals. It provides general operating instructions and training requirements for CDCS operators.

- Section 511 describes the procedures to be followed in receiving and transmitting classified matter, including the mailing, hand carrying, and electronic transmission of classified matter.

- Section 512 describes the procedures for identifying the mailing addresses to be used in sending classified matter to facilities operated by DOE and other government agencies.

- Section 513 deals with the use of Express Mail Services to send and receive classified matter.

- Section 514 describes the procedures and equipment required to properly destroy classified matter.

Section 501
Classified Matter Protection and Control
Roles and Responsibilities

Individuals granted security clearances by the U.S. Government are responsible for protecting the classified matter with which they are entrusted. This responsibility means the person has a duty to control access to the information and ensure that it is not disclosed to unauthorized persons. There is a two-part test to determine whether classified information can be shared with another person:

1) Does the other person have a security clearance that permits access to the classified matter?
2) Does the other person have "need-to-know" for that classified information?

If the answer to either question is "no," the classified information cannot be disclosed to the other person.

Numerous rules and procedures apply to the protection and control of classified matter. This section describes the basic responsibilities of persons entrusted with classified information; subsequent sections describe specific protective measures in much greater detail.

The U.S. Department of Energy (DOE) Headquarters (HQ) Classified Matter Protection and Control (CMPC) Program is managed by the Office of Information Security (AU-42).

HQ Implementation Procedures

HQ CMPC Program Manager:

The Director of the Office of Headquarters Security Operations (AU-40) has appointed a single individual within AU-42 to serve as the HQ CMPC Program Manager. The CMPC Program Manager is responsible for developing HQ-wide CMPC procedures to implement the requirements of applicable laws, Executive Orders, and DOE directives.

Comprehensive Security Briefing:

Title 32 CFR 2001 and DOE policy require that all individuals who are authorized to access classified information must receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable of their responsibilities and applicable requirements. The instruction is provided in a Comprehensive Security Briefing. The individual is notified of the requirement to complete the Comprehensive Security Briefing, and provided the necessary link via email from the DOE badge office prior to being issued their DOE badge (see Chapter 10, Security Awareness Program for more information). Upon verification

of completion of the briefing by the servicing badge office, the badge office issues the employee his/her security badge reflecting his/her clearance level and before he/she is authorized access to classified information, a Limited Area (LA), or a Vault Type Room (VTR). The Comprehensive Security Briefing describes the requirements for proper handling and storage of classified matter, access control procedures for LAs and VTRs, escort requirements, penalties for mishandling classified information, controlled articles, and other topics associated with the protection of classified matter.

Upon proof of completion of the Comprehensive Security Briefing, the employee is required to read and sign SF-312, *Classified Information Nondisclosure Agreement*, with the briefing official signing as the witness. The signed SF-312 documents the employee's completion of the Comprehensive Security Briefing. Any employee who fails to complete the SF-312 will have his/her access authorization terminated and will be denied access to classified matter. The badge offices maintain records of who completed the briefing and their signed SF-312s, which are retained for a period of 70 years.

Annual Security Refresher Briefing:

All HQ employees, both Federal and contractor, with a Q or L security clearance must complete an Annual Security Refresher Briefing (ASRB). This computer-based briefing summarizes DOE security requirements, the threat to national security interests, and other matters concerning the proper handling and storage of classified matter. Personnel who are required to take the briefing receive an automated email message advising them how to access the briefing, establishing a required completion date, and advising how to print a completion certificate. The automated system has an integrated audit capability to track who has completed the briefing. HSOs are required to monitor who within their element has not completed the briefing and take action to ensure their element achieves a 100% completion rate. Failure to complete the ASRB may impact the employee's access to DOE facilities and classified material as well impact his/her ability to maintain a security clearance.

Specialized CMPC Training:

Title 32 CFR 2001, Section 2001.71 requires specialized CMPC security training for security managers, security specialists, and all other personnel whose duties significantly involve the handling of classified information. In addition, for HQ positions, specialized training is required for HSOs, Alternate HSOs, and HSO Representatives representing elements that handle classified information; CDCS operators; classified document couriers; and mailroom personnel. This training should be completed before or concurrent with the date the employee assumes any of the positions listed above, but in any case, no later than six months from that date. Note: HSOs are required to complete this training within two years of appointment to HSO duties.

It is the responsibility of the Head of Element to determine which of the element's employees require specialized CMPC training and ensure that the identified employee(s) complete the training. Note that specialized training requirements may change (e.g., when

an employee is assigned new security responsibilities or when an employee is involved in a security incident regarding the mishandling of classified matter).

The HQ CMPC Program Manager is responsible for developing specialized CMPC training courses and making the training available to the HQ Federal and contractor population.

The HQ CMPC Program Manager has developed and conducts specialized training courses for HQ personnel with specific security responsibilities. For example, there are training courses in:

- Classified Matter Protection and Control Overview
- Classified Document Control Station Operations
- Congressional Courier Operations
- Classified Document Courier Operations
- Hand Carrying Classified Matter

Upon request, the HQ CMPC Program Manager also develops and presents individualized CMPC courses for HQ organizations with specified requirements.

Specialized training courses are available throughout the year. Most of the courses are offered in person or virtually via WebEx or Microsoft Teams. HSOs are advised when many of these training opportunities are available and may nominate their organizational personnel to attend. Additionally, organizational management, or the HSO, may submit requests for specialized CMPC training at any time during the year.

Other CMPC Training:

The DOE National Training Center (NTC) in Albuquerque, New Mexico offers a variety of specialized CMPC courses. The HQ element is responsible for sponsoring and funding the attendance, travel, and other actions associated with their personnel attending NTC courses. NTC delivers their training both in Albuquerque and in a variety of other ways, including computer-based training (eLearning), correspondence courses, and Mobile Training Teams. Introduction to Classified Matter Protection and Control (NTC-ISC-121DE) is available on DOE Learning Nucleus for all DOE and DOE-Contractor personnel. A link to the NTC website and course catalog is included in the Helpful Websites subsection below. The NTC website fully describes NTC's course offerings, schedule, and points of contact.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, contact the Office of Information Security or call (301) 903-9990 or (202) 586-4487

Helpful Websites

National Training Center Website

DOE LMS Information and Registration

Section 502
Classification

DOE Order 475.2B, *Identifying Classified Information*, establishes DOE's program for classifying and declassifying information and specifies requirements and responsibilities for implementing this program. This order also describes the procedures for classifying and declassifying information, documents, and material, as well as the associated processes, such as training, classifier appointments, and authority descriptions. These standard procedures are in use throughout DOE HQ.

HQ Implementation Procedures

- HQ elements that have employees who generate classified information, documents, or material must appoint a Classification Representative to assist individuals within the element implement the requirements in DOE Order 475.2B. To identify an element's Classification Representative, email the Office of Classification's outreach program or call 301-903-7567.

- Any document that is in a classified subject area and that might contain classified information must be reviewed by a Derivative Classifier (DC) with appropriate authority.

- Before a classified document can be declassified or have classified information removed (redacted), it must be reviewed by a Derivative Declassifier with the appropriate authority.

- When a document needs to be classified or declassified, contact the element's Classification Representative or the Office of Classification's outreach program to determine who the DCs or Derivative Declassifiers are within the element.

- When a document was issued as Unclassified or at too low a level or category, its classification must be upgraded. In such a case, the DC should notify the Office of Classification (AU-60) immediately after making the upgrade.

- All documents in a classified subject area that are intended for public release, or for submittal to Congress as Unclassified, must be reviewed by AU-60 or the NNSA Office of the Associate Administrator for Defense Nuclear Security (NA-70).

- All HQ Employees are encouraged and expected to challenge the classification of information, documents, or material believed to be improperly classified. Resolving the challenge locally is encouraged; however, employees have the right to submit the challenge directly to the Director, Office of Classification at any time. Under no circumstances is the employee subject to retribution for making a challenge.

Points of Contact

For information about the Classification Program, contact (301) 903-7567 or email the Office of Classification's outreach program.

Helpful Websites

The Office of Classification's website is at: Office of Classification website

To view the *DOE CMPC Marking Resource*, go to:
CMPC Marking Resource

Section 503
Types of Classified Matter

This section describes the levels and categories of classified matter in use throughout the U.S. Government and the types of classified information that are unique to, or controlled by, DOE and/or DOE HQ.

Access to Classified Information

Only personnel who have an appropriate security clearance and need-to-know are permitted to access classified matter. Additional access limitations may be indicated for classified matter through the use of control caveats or special control markings.

HQ Implementation Procedures

Classified information is defined as any information or material that has been determined by the U.S. Government, pursuant to an Executive Order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security. There are four categories and three levels of classified matter. Categories and levels of classified information may exist in various forms, such as documents, emails, photos, matter, media, parts, weapons systems, or verbal disclosure.

Classified Matter is defined as anything in physical form that contains or reveals classified information such as: Classified equipment, components, parts, tooling gauges, liquids, powder, scrap, molds, packaging container inserts…etc.

Levels of Classified Information:

- Top Secret (TS) – The **Top Secret** classification level is applied to information whose unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.
- Secret (S) – The **Secret** classification level is applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.
- Confidential (C) – The **Confidential** classification level is applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security.

Categories of Classified Information:

- Restricted Data (RD) – Classified information that concerns (1) the design, manufacture, or utilization of atomic weapons; (2) production of special nuclear material; or (3) the use of special nuclear material in the production of energy, except

for that information that has been declassified, or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954

- Formerly Restricted Data (FRD) – Classified information concerning the military utilization of atomic weapons that has been removed from the RD category under Section 142d of the AEA and remains classified

- National Security Information (NSI) – Classified information that has been determined under Executive Order 13526, *Classified National Security Information,* or any predecessor Executive Order, to require protection against unauthorized disclosure

- Transclassified Foreign Nuclear Information (TFNI) – Classified information concerning foreign nuclear programs that has been removed from the RD category under Section 142e of the AEA.

Caveats and Special Controls (for classified matter):

Caveats and special control markings identify special handling or dissemination requirements and help describe the type of information involved, or who distributed or originated the information.

1. Caveats:
   - Foreign Government Information (FGI) – See Section 504, Classified Foreign Government Information, for more detailed information
   - Director of National Intelligence (formerly Director of Central Intelligence) – These markings are restricted, except as noted, to intelligence matter:
     - No Foreign Dissemination (NOFORN); may also be used on Naval Nuclear Propulsion Information (NNPI)
     - Originator Controlled Information (ORCON)
     - Proprietary Information (PROPIN)
     - Authorized for Release To (REL TO); usually used in conjunction with NOFORN
     - Releasable by Information Disclosure Official (RELIDO)

       NOTE: No Dissemination to Contractors (NOCONTRACT) and Warning Notice: Sensitive Intelligence Methods or Sources Involved (WNINTEL) designations are obsolete but remain applicable on the documents that bear these markings until such time as the document is re-reviewed and re-marked.

2. Special Control Requirements:
   - North Atlantic Treaty Organization (NATO)
     - COSMIC TOP SECRET
     - ATOMAL
     - CRYPTO.

- Weapon Data
  - Sigma Category (SIGMA) (14; 15; 18; 20)
  - Critical Nuclear Weapons Design Information (CNWDI) – Department of Defense designation TS or S/RD revealing the theory of operation or design of the components of a thermonuclear implosion-type fission bomb, warhead, demolition munition, or test device.
- Naval Nuclear Propulsion Information – NNPI may be classified or unclassified and must also be annotated NOFORN.
- Special Category (SPECAT)
- Dissemination and Reproduction Notices
  - FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY
  - REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (301) 903-9990 or (202) 586-4487

Helpful Websites

To view DOE Order 471.6, *Information Security,* go to:
DOE Order 471.6 Admin Chg. 3, Information Security

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

Section 504
Classified Foreign Government Information

This section describes DOE HQ procedures for identifying and handling FGI. FGI requires protection pursuant to an existing treaty, agreement, bilateral exchange, or other obligation. FGI is defined as information that is:

- Provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
- Produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any elements thereof, requiring that the information, the arrangement, or both are to be held in confidence; or
- Received and treated as "Foreign Government Information" under the terms of a predecessor order.

NOTE: North Atlantic Treaty Organization (NATO) information is FGI but must be safeguarded in compliance with NATO procedures (United States Security Authority for NATO Affairs [USSAN] 1-07).

HQ Implementation Procedures

General Requirements:

All FGI is classified national security information as defined by Executive Order 13526. The release or disclosure of classified FGI to any third country must have the prior consent of the originating government if required by treaty, agreement, bilateral exchange, or other obligation.

FGI must retain its original classification markings or be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Consult the *DOE CMPC Marking Resource* Foreign Government Markings Table.

TS/FGI, S/FGI, and C/FGI should be stored separately from other classified information, either in a separate approved classified repository or in separate drawers in a GSA-approved security container.

If the original markings in the foreign government documents are readily recognizable as relatable to a U.S. classification requiring special protection and control, the documents do not require re-marking.

If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a DC, and an equivalent U.S. classification must be applied.

Review by a DC is not required to apply a U.S. classification level that provides at least an equivalent level of protection to a document or material classified by the foreign government. Documents generated by DOE personnel that contain FGI must be reviewed by a DC with appropriate authority.

An incoming FGI classified document is considered to be classified in its entirety. Portion markings are not required to be added to the document; however, portion marking is required when a newly created FGI document contains U.S. information.

Accountability of FGI:

- **TS/FGI** – All TS/FGI is accountable. Reproduction requires the consent of the originating government. Destruction must be accomplished by two individuals and a Destruction Certificate must be completed by both individuals to record the actual destruction.
- **S/FGI** – S/FGI requires modified accountability. Records must be kept for receipt, external transfer, destruction, and reproduction. Unless prohibited by the originator, S/FGI may be reproduced, and reproduction must be recorded unless the requirement is waived by the originator. Destruction must be accomplished by two individuals, and a Destruction Certificate must be completed by both individuals to record the actual destruction.
- **C/FGI** – Accountability records need not be retained for C/FGI unless the originator establishes a requirement for such records.

Confidential/Foreign Government Information – Modified Handling Authorized:

For some FGI, the foreign government protection requirement may be lower than the protection required for U.S. Confidential information; however, the foreign government still expects that the information will be held in confidence. In such cases, the document is handled as Confidential – Modified Handling Authorized (C/FGI-MOD), and so marked on the first page. A DOE F 470.9, *C/FGI-MOD Cover Sheet*, must be used; this form is to be used only on C/FGI-MOD documents. The country of origin must be indicated at the bottom of the cover sheet. The marking on the first page of the document must be as follows:

This document contains (*insert name of country*) (*insert NSI classification level*) information to be treated as CONFIDENTIAL – MODIFIED HANDLING AUTHORIZED

Access to C/FGI-MOD does not require an access authorization but does require need-to-know in performance of official duties.

C/FGI-MOD is national security information classified under Executive Order 13526. Uncleared individuals given access to C/FGI-MOD must be provided appropriate handling instructions, via a briefing from the manager responsible for the program involving the C/FGI-MOD, or via written instructions on an approved C/FGI-MOD coversheet, DOE F 471.2.

Information systems that store and/or process C/FGI-MOD cannot be accessed or serviced by foreign nationals.

When not in use, C/FGI-MOD must be stored in a locked receptacle (e.g., file cabinet, desk, bookcase) that is accessible only to persons who need-to-know the information to perform their official duties. Such persons must prevent unauthorized disclosure or access by unauthorized persons.

C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties.

C/FGI-MOD must be transmitted in the same manner as classified matter unless this requirement is waived by the originating foreign government.

C/FGI-MOD information must be destroyed in the same manner as classified information (see Section 514).

Point of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (301) 903-9990 or (202) 586-4487

Forms/Samples/Graphics

DOE Form 471.2, *C/FGI-MOD Cover Sheet* (for a copy of this form go to DOE Form 471.2, C/FGI-MOD Cover sheet)

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

Section 505
Marking Classified Matter

This section describes DOE HQ procedures for marking classified matter. Regardless of date or agency of origin, classified matter must be marked to indicate at least the classification level and category (if RD, FRD, or TFNI). All classified documents dated **after** April 1, 1996, must be marked in accordance with directives in place at the time of origin.

HQ Implementation Procedures

General Procedures:

The markings that are common to all classified documents include:

- Classification level
- Classification category (if RD, FRD, or TFNI)
- Caveats (special markings) if applicable
- Authorized classifier information
- Originator identification
- Title/Subject marking
- Unique identification numbers (for accountable matter only)
- Portion marking (for documents containing NSI or TFNI).

Any deviation from these requirements will be specifically stated. Consult the *DOE CMPC Marking Resource* for details on how to properly mark classified matter in its various forms.

NOTE 1: DOE conforms to and does not exceed the requirements of the Federal Government, implemented by the U.S. Government Information Security Oversight Office (ISOO), for marking classified documents. If a classified document is originated by DOE, it must be correctly marked in all respects. If incompletely marked, the originating office should be consulted to resolve all discrepancies. Classified documents received by DOE from Other Government Agencies (OGAs) are often not marked in accordance with national standards. To ensure proper protection of such documents, these documents must be marked with the overall classification level and protected with the appropriate cover sheet for classified information. Resolution of OGA deficiencies and/or continuing patterns of deficiencies should be handled through the CMPC Program Manager, AU-42.

NOTE 2: All classified documents (other than Working Papers or draft documents – see below) must contain a classification authority block that identifies the DC who reviewed the document, the guide or source the decision was based upon, and the declassification date or event for NSI documents. This classifier's

identification is recorded on the face of each classified document. A DC must make the classification determination for the original copy of each document. Any change to any classified document requires a DC review. The placement of a DC's name on a classified document without the DC's direction or authorization is illegal and will result in an official inquiry and/or investigation. Consult DOE Order 475.2B for additional information on identifying classified information.

NOTE 3: All NSI documents and all page changes to NSI documents created after April 1, 1997, must be portion marked.

Classified Cover Sheets:

All classified documents must have an appropriate cover sheet (Top Secret, Secret, or Confidential) attached to the face of the document depicting the classification level of the protected classified matter whenever that document is outside a GSA-approved security repository. Additionally, the back of all classified documents must also have an appropriate cover sheet attached or, if the back of the last page is blank, the overall highest classification level of the document may be marked at top and bottom of the page.

Marking Standard Form 700, Security Container Information:

Special considerations are in place for marking SF-700, *Security Container Information*, the three-part form used to record safe and door combinations. See Section 507, Storage of Classified Matter, for instructions on how to mark SF-700s.

Marking Electronic Files:

Individuals are responsible for ensuring that classified electronic files (e.g., e-mail, documents) that are transmitted or shared outside the individual's exclusive domain (i.e., the individual's computer) are reviewed and properly marked. More specifically, individuals are responsible for including all of the classified markings that are required to appear on paper copies of documents when classified documents (files) are in electronic form, including text within a database, data within a spreadsheet, and web-based documents (HTML, ASCII text file, etc.). Additional guidance is provided in 32 CFR Section 2001.23.

The required markings include:

- Portion marking in the body of all NSI documents
- Classification level and category markings (if RD, FRD, or TFNI) at the top and bottom of each page, or at the beginning and end of the actual text if header and footer markings are impractical (e.g., e-mail) or not available with the software used
- Caveats, if any
- Title/Subject markings (regardless of category)
- Classification authority, with the name and title of the classifier, classification

authority, and declassification instructions for NSI only.

NOTE: Portion marking is not required for documents/files containing RD or FRD.

Examples of electronic files that must be marked include, but are not limited to:

- Word processing, database, spreadsheet, and HTML documents
- E-mail and/or attachments to e-mail
- Files that are shared in a peer-to peer network (two or more personal computers directly connected to each other)
- Files that are posted to a classified network server for access by other than the originator
- Electronic files that are hand transmitted (physically handing media containing the file to another person).

Marking E-Mail Messages:

Consult 32 CFR Section 2001.23.

Note: Email Derivative Classifier (EDC) training is required for all Headquarters Federal and contractor employees with access to C-LAN, JWICS, SIPRNet or ESN/NSN. EDC training ensures that all C-LAN, SIPRNet, JWICS, or ESN/NSN users are trained and have authority to classify and mark email. Refer to the Classification Training Institute for more information.

Classified Working Papers and Drafts:

Classified Working Papers and drafts are considered to be interim production stages toward the generation of a permanent document and are usually created during research or note taking at classified meetings, seminars, classes, symposiums, or conferences. Working papers (generated electronically and on paper) must be:

- Marked with the date created
- Protected and marked in accordance with the highest potential classification level, category (if RD, FRD, or TFNI), and caveats if applicable
- Annotated with "Working Paper" or "Draft" on the first page of the text
- Protected by the approved classified cover sheet (when the electronic version is printed or when removed from a GSA approved security container)
- Destroyed when no longer needed
- Accounted for (if required) and controlled and marked in the manner prescribed for a finished document of the same classification when the working papers are:
    - Released by the originator outside the specific HQ element activity or office;
    - Retained for more than 180 days from the date of origin; or
    - Filed permanently.

Working Papers/drafts that are frequently updated as part of a project or study, commonly referred to as "living" documents, may be considered to be (re)originated upon each change. The date of each revision, addition, or change must be clearly indicated on the document. One suggestion is to line out (but not obliterate) the date of the last change and insert the new date of the current revision, addition, or change on the document itself. Another option is to attach a change sheet to the front of the document, listing the date of each change. Once re-dated, the 180-day limit for retention starts over again.

Classified drafts and working paper documents retained past 180 days, without being reviewed for classification and marked as final documents, are improperly marked documents. Failure to comply with the requirements for reviewing and marking such documents may result in the issuance of a security infraction. Such documents must either be destroyed prior to day 181, returned to the originator for proper classification marking prior to day 181, or submitted to your organization's classification representative or derivative classifier for proper classification review, determination and marking, as appropriate.

Classified drafts and working papers are often difficult to identify when they are stored and commingled with other classified documents in a security container. As such, they should be kept together in a separate "Draft" or "Working Paper" file inside the control drawer of an approved security container. The file should be reviewed monthly by the document custodian or security container custodian to ensure no draft or working paper document is retained past 180 days without being properly reviewed and marked as a final document.

When the final classification of a draft or working paper must be sent outside the office of origin for a classification review and determination, it must be marked:

DRAFT - NOT REVIEWED FOR CLASSIFICATION

NOTE: This marking does not preclude the need to mark and protect the draft or working paper at the highest estimated classification level and category pending review.

If the classification determination cannot be made locally, a Document Undergoing Classification Review cover sheet (see Additional Resources) may be appropriately completed and attached to the draft document, with an appropriate classified cover sheet on top. This option should be used only when the DC within the organization cannot make the final classification determination for the document. This cover sheet does not preclude the need to mark the working paper/draft with the highest possible classification level and category.

Notes taken during a meeting, conference, etc., that involves classified information, or a classified subject area are to be considered classified working papers and must be protected and marked with the highest potential classification level and category, and with appropriate caveats, as applicable. A review by a derivative classifier is required if the notes become a

final document, are filed permanently, or are retained longer than 180 days. Transmission of notes of uncertain classification must be in accordance with Section 511, Receipt and Transmission of Classified Matter.

For detailed information on marking working papers and drafts, consult the *DOE CMPC Marking Resource*, accessible through the Helpful Websites subsection below.

Points of Contact

For questions about the HQ CMPC Program, contact the Office of Information Security or call (301) 903-9990 or (202) 586-4487

Additional Resources

32 CFR Section 2001.23

Document Undergoing Classification Review Cover Sheet (a clean, .pdf version of this cover sheet may be requested by sending an e-mail to "AU-42 Operations").

Helpful Websites

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

To view EDC and other marking training, go to:

Classification Training Institute

32 CFR 2001.23

Title 32: National Defense

PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION
Subpart C—Identification and Markings

§ 2001.23 Classification marking in the electronic environment.

(a) *General. C*lassified national security information in the electronic environment shall be:

(1) Subject to all requirements of the Order.

(2) Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, "Classified By," "Derived From," "Reason" for classification (originally classified information only), and "Declassify On."

(3) Marked with proper classification markings when appearing in an electronic output (*e.g.,* database query) in which users of the information will need to be alerted to the classification status of the information.

(4) Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information.

(5) Prohibited from use as source of derivative classification if it is dynamic in nature (*e.g.,* wikis and blogs) and where information is not marked in accordance with the Order.

(b) *Markings on classified e-mail messages.*

(1) E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail shall reflect the classification of the header and body of the message. This includes the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings shall be included in the first line of text and at the end of the body of the message after the signature block.

(2) Classified e-mail shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (*i.e.,* link) to another document shall be portion marked

based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.

(3) A classified signature block shall be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.

(4) Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(5) For a classified e-mail, the classification authority block shall be placed after the signature block, but before the overall classification marking string at the end of the e-mail. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) When forwarding or replying to an e-mail, individuals shall ensure that, in addition to the markings required for the content of the reply or forward e-mail itself, the markings shall reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(c) *Marking Web pages with classified content.*

(1) Web pages shall be classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of information to which the web materials link shall also be marked based on its own content.

(2) The overall classification marking string for every web page shall reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation is utilized, a text equivalent of the overall classification marking string shall be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified Web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

(5) Classified Web pages shall include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides shall carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure shall be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

(d) *Marking classified URLs. U*RLs provide unique addresses in the electronic environment for web content and shall be portion marked based on the classification of the content of the URL itself. The URL shall not be portion marked to reflect the classification of the content to which it points. URLs shall be developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark shall be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL. An example may appear as:

http://www.center.xyz/SECRET/filename_(S).html

http://www.center.xyz/filename2_(TS).html

http://www.center.xyz/filename_(TS//NF).html

(e) *Marking classified dynamic documents and relational databases.*

(1) A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.

(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings shall be applied to and displayed on the document. If such a mechanism does not exist, the default should be the highest level of information in the database and a warning shall be applied at the top of each page of the document. Such content shall not be used as a basis for derivative classification. An example of such an applied warning may appear as:

This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

(3) This will alert the users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users shall be encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as classification guides and points of contact shall be established to assist with these inquiries.

(4) Users developing a document based on query results from a database must properly mark the document in accordance with §2001.22. If there is doubt about the correct markings, users should contact the database originating agency for guidance.

(f) *Marking classified bulletin board postings and blogs.*

(1) A blog, an abbreviation of the term "web log," is a Web site consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.

(2) The overall classification marking string for every bulletin board or blog shall reflect the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.

(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) The overall classification marking string for the bulletin board posting, blog entry, or comment shall reflect the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings shall be entered manually or utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.

(5) Bulletin board postings, blog entries, or comments shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(g) *Marking classified wikis.*

(1) Initial wiki submissions shall include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. Systems shall provide a means to log the identity of each user, the changes made, and the time and date of each change.

(3) Wiki articles and entries shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(h) *Instant messaging, chat, and chat rooms.*

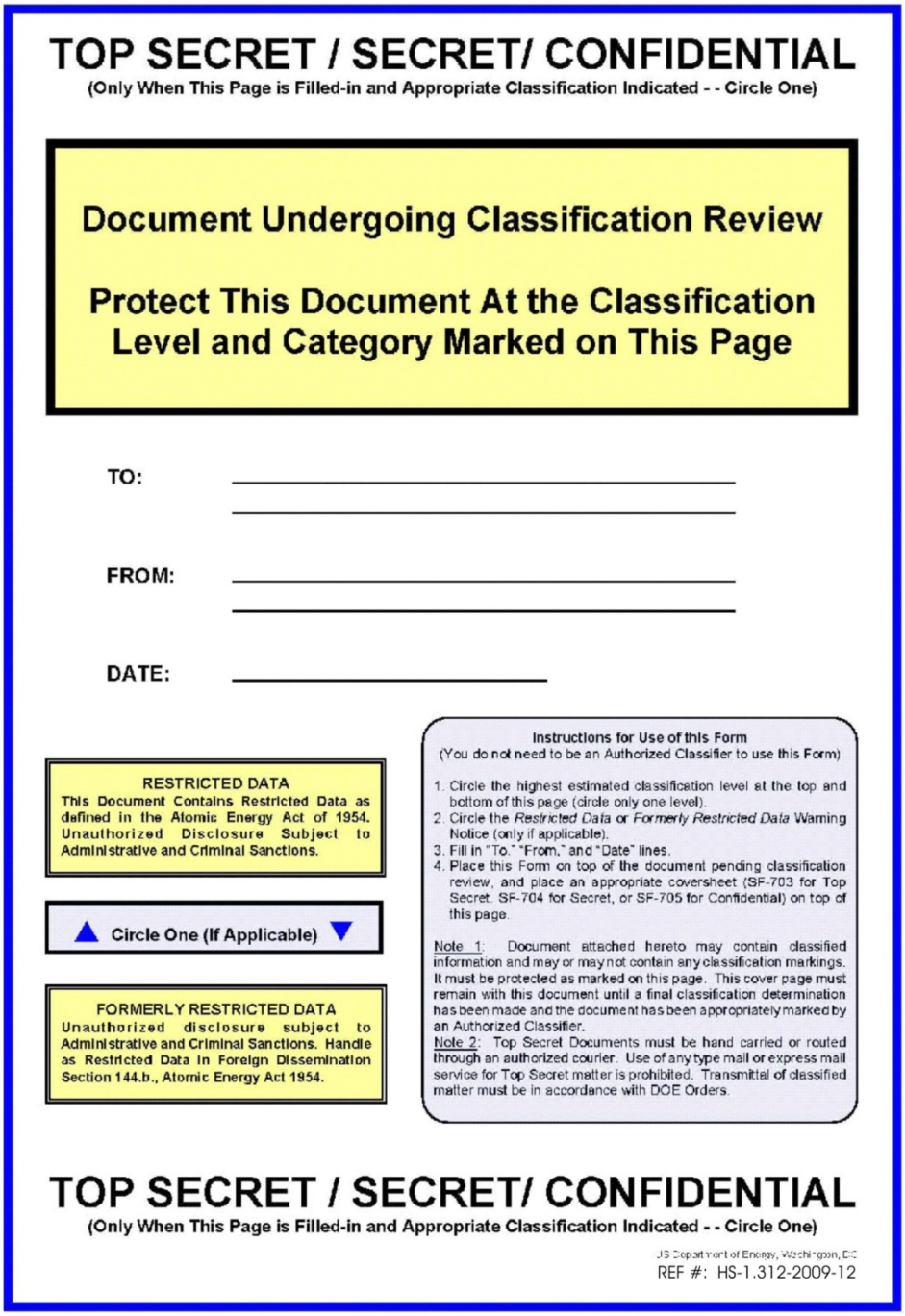
(1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or

printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string shall also appear.

(2) Chat rooms shall display system-high overall classification markings and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.

(i) *Attached files*. *W*hen files are attached to another electronic message or document, the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with §2001.24(b).

Document Undergoing Classification Review Cover Sheet



TOP SECRET / SECRET/ CONFIDENTIAL

(Only When This Page is Filled-in and Appropriate Classification Indicated - - Circle One)

Document Undergoing Classification Review

Protect This Document At the Classification Level and Category Marked on This Page

TO: _____

_____

FROM: _____

_____

DATE: _____

RESTRICTED DATA

This Document Contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized Disclosure Subject to Administrative and Criminal Sanctions.

▲ Circle One (If Applicable) ▼

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.

Instructions for Use of this Form

(You do not need to be an Authorized Classifier to use this Form)

1. Circle the highest estimated classification level at the top and bottom of this page (circle only one level).
2. Circle the *Restricted Data* or *Formerly Restricted Data* Warning Notice (only if applicable).
3. Fill in "To," "From," and "Date" lines.
4. Place this Form on top of the document pending classification review, and place an appropriate coversheet (SF-703 for Top Secret, SF-704 for Secret, or SF-705 for Confidential) on top of this page.

Note 1: Document attached hereto may contain classified information and may or may not contain any classification markings. It must be protected as marked on this page. This cover page must remain with this document until a final classification determination has been made and the document has been appropriately marked by an Authorized Classifier.

Note 2: Top Secret Documents must be hand carried or routed through an authorized courier. Use of any type mail or express mail service for Top Secret matter is prohibited. Transmittal of classified matter must be in accordance with DOE Orders.

TOP SECRET / SECRET/ CONFIDENTIAL

(Only When This Page is Filled-in and Appropriate Classification Indicated - - Circle One)

US Department of Energy, Washington, DC

REF #: HS-1.312-2009-12

This page intentionally left blank.

Section 506
Protection of Classified Matter in Use

This section describes DOE HQ policies and procedures pertaining to the protection of classified matter while it is in use. When it is not actually being used, it must be stored within a security container or a VTR that is approved for open storage of classified matter. (See Section 507, Storage of Classified Matter).

HQ Implementation Procedures

All persons who access classified matter must possess a security clearance commensurate with the classification level and category of information being accessed and need-to-know for that information in the performance of their official duties. Classified matter will be protected at all times and, as a general rule, will be accessed for use only in approved LAs or VTRs. However, there are exceptions to the rule. See Chapter 2 of the HQFMSP, Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs, for information on establishing a Temporary Limited Area for the review of classified information.

> *NOTE: Refer to Chapter 2 (HQFMSP), Page 2-13, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussions, if classified discussions are anticipated outside a LA or VTR.*

Emergency Situations:

If the emergency is life threatening (e.g., explosion, fire), the health and safety of the individual takes precedence over the need to secure classified matter in accordance with normal storage requirements.

Depending on the intensity and urgency of the emergency situation, classified matter should be secured in the most expeditious way possible: in an accessible security container (preferred method), file cabinet, desk, alternate areas within the facility, etc.

No policy can specify employee actions for every conceivable scenario. **Use your best judgment while protecting both your health and safety and the classified matter.**

These actions must be taken after the emergency:

- All unsecured classified matter must be located, accounted for, and returned to proper storage.
- Security containers and VTRs must be inspected to ensure that they have not been compromised.

Fire and Evacuation Drills:

Fire and evacuation drills must be carried out as realistically as possible so that individuals know how to respond during a real emergency. Therefore, individuals should handle all classified information as described above, regardless of whether the emergency is real or a practice drill.

Emergency Response Personnel:

In an emergency involving an imminent threat to life or national defense, emergency personnel who are not otherwise routinely eligible for access to classified information may be granted emergency access to security areas and/or classified information. Examples include providing law enforcement personnel classified information about an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient. The following actions must be taken if such an intentional release of classified information is required:

- The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum required to achieve the intended purpose.

- The information must be transmitted over approved channels using the most secure and expeditious method.

- The recipient must be informed of what specific information is classified and the protection requirements for the information.

- The recipient must be briefed on his/her responsibilities for not disclosing the information and must sign a nondisclosure agreement.

- The information must remain in the physical custody of an authorized Federal Government entity in all but the most extraordinary circumstances.

Within 72 hours of the disclosure of classified information or at the earliest opportunity that the emergency permits, but no later than 30 days after the release of classified information to an emergency responder, the official making the disclosure decision must report the disclosure. The report must include:

- A description of the disclosed information
- A list of individuals to whom the information was disclosed
- A description of how the information was disclosed and transmitted
- The reason for the emergency release
- How the information is being protected.

The disclosure must be made to:

- Director (AU-42) and the NNSA Associate Administrator for Defense Nuclear Security (NA-72) when RD or FRD has been released

- The Director (AU-40) when NSI or TFNI has been released.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call, (202) 586-4487, (301) 903-9990 or (301) 903-2644.

This page intentionally left blank.

Section 507
Storage of Classified Matter

This section describes DOE HQ policies and procedures pertaining to the storage of classified matter. In summary, all classified matter must be stored within a security container in an LA or VTR, or in a VTR approved for open storage of classified matter.

HQ Implementation Procedures

Classified matter must be stored at all times in a designated LA or VTR that has been approved and certified by AU-40 (see Chapter 2 (HQFMSP), Establishing, Maintaining, and Deactivating LAs, and VTRs). Unless AU-40 has certified a VTR for the open storage of classified matter, all classified matter must be stored in GSA-approved containers located within approved and certified LAs or VTRs. GSA containers and VTRs in use for the storage of classified matter must be equipped with an, X-07, X-08, X-09, and X-10 series electromechanical combination lock. HQ facilities are required to utilize the X0 series combination locks on security containers

NOTE: Money, firearms, medicines, controlled substances, and other items of monetary value susceptible to theft shall not be stored in the same security containers used to store classified matter.

In general, TS matter shall be stored in a locked GSA-approved security container (i.e., closed storage) within a designated LA or VTR. The following types of classified storage facilities must additionally be protected by an intrusion detection system certified by AU-40:

- A VTR approved and certified for the open storage of classified matter
- An approved and certified VTR that opens into a Property Protection Area
- A LA or VTR with closed storage of TS matter.

Open storage of TS matter within rooms that meet VTR requirements **may be authorized** (see Chapter 2 (HQFMSP), Establishing, Maintaining, and Deactivating LAs, and VTRs) **on a case-by-case basis** based on storage requirements that cannot be reasonably met by an alternative approved method (e.g., GSA-approved storage container). Requests for approval of open storage of TS matter must be predicated on a programmatic requirement for open storage, not as "a matter of convenience."

NOTE: At HQ, TS matter can be stored only in the Forrestal and Germantown buildings.

Responsibilities for Security Containers and Vault-Type Rooms:

Personnel who access security containers and VTRs are responsible for protecting classified matter at all times and for locking classified matter in appropriate security containers whenever it is not in use or under the direct supervision of authorized persons. These individuals must ensure that unauthorized persons do not gain access to classified matter. In areas approved for open storage, classified matter need not be stored in a security container (the open storage level/category authorized is indicated in the specific room or facility certification).

Repository Opening Procedures:

To open the door to a VTR:

- Deactivate the premise alarm system (if applicable).
- Dial the combination and open the lock.
- Record the opening on the SF-702, *Security Container Check Sheet*.
- After opening a VTR equipped with an X0 series combination door lock, check the life-safety switch (see diagram below); it should be pushed ***in*** to prevent accidental locking.

To open a security container (safe):

- Dial the combination and open the lock.
- Record the opening on the SF-702.

NOTE: The sole custodian of a security container is not required to record each opening and closing of the container throughout the day. In such cases, the appropriate information should be recorded on the SF-702 the first time the container is opened that day. The container may be opened and closed as necessary without further record keeping. At the end of the day, information should be recorded indicating the final closing of the container for that day. If two or more persons have authorized access to the container, each opening and closing must be duly recorded.

Repository Closing Procedures:

To close and secure a security container (safe):

- Visually check the immediate area and top of the container for any classified matter that may have been left unattended and put it in the appropriate storage location.

- Close all safe drawers and lock the X0 series combination lock by turning the dial at least three full rotations in the counterclockwise direction and then

turning the dial at least one full rotation in the opposite, clockwise direction.

- Verify that all the container drawers are locked by attempting to turn the handle and simultaneously attempting to pull the drawer open. Then check each auxiliary drawer by activating its thumb release and attempting to pull the drawer open.

NOTE 1: If the dial cannot be turned in either direction, the container bolt locking mechanism has not engaged into the locking mode (e.g., a drawer may not be fully closed, or matter may be jammed in the drawer path).

NOTE 2: If the dial stops turning when turned in the clockwise direction, the container and/or lock is not locked.

- Record the closing/checking action on the SF-702.

- At the end of the workday, complete the SF-701, *Activity Security Checklist* that is explicitly tailored to the specific room, area, or activity. The SF-701 is to be posted inside the area being protected.

To close and secure the door to a VTR:

- Ensure that the life safety switch is pulled ***out*** (the off position) to permit activation of the door lock.

- With the door open, rotate the combination lock dial at least one turn to the left (counterclockwise); there will be a slight resistance to turning until the locking mechanism has engaged. *NOTE: If the dial will not turn counterclockwise, the life safety switch is engaged (on).*

- Exit the room and close the door securely; the locking mechanism will snap into and engage the strike on the door jamb.

- Rotate the combination lock dial one full turn to the right (clockwise). If the dial stops turning when turned in the clockwise direction, the XO series lock is not locked.

- Check that the door is fully secured:

  - If the VTR door **is not** equipped with an access control mechanism (cipher lock, card reader, etc.), attempt to open the door without activating the XO series combination lock. If the door **is** equipped with an access control mechanism (cipher lock, card reader, TESA® lock, keyed door knob, etc.), the access control must be activated with an attempt to enter the VTR without activating the XO series combination lock.

  - On a GSA-approved vault door, attempt to turn the handle release mechanism and open the vault door.

  - On a VTR door containing a mechanical or electromechanical cipher lock in addition to the XO series lock, activate the cipher code and/or card or key and attempt to open the door after securing the XO series door lock.

- Activate the premise alarm. *NOTE: Within HQ facilities, premise alarms for VTRs, when so equipped, must be activated whenever the facility is unoccupied*.

- Record each closing/checking action on the SF-702, which must be posted on the outside of the door to the VTR.

In case of a security system malfunction (e.g., door will not close or lock, or alarm system, if applicable, will not set up), do not leave classified matter unattended. Contact the element HSO, protective force personnel, or appropriate management official to determine a course of action, including an alternative way to secure the classified matter.

Possible Forced Entry into Security Containers and Vault-Type Rooms:

If there is any indication of forced entry into a security container or VTR, the individual making the discovery must notify the HQ protective force who must, in turn, follow the plan of action detailed in HQ protective force post orders. The discovery must also be reported to the HSO responsible for the LA or VTR so the HSO can report the discovery as a security incident (see Chapter 11, *Incidents of Security Concern*). The area must remain protected, and every effort must be made to leave the area untouched or undisturbed until a decision to proceed has been granted by AU-40. Appropriately cleared management or HSO personnel must stand by the area until the potentially compromised classified matter is secured and/or until released by AU-40. The individual discovering the forced entry must stand by until he/she has given a statement to the DOE HQ protective force. A complete inventory of the contents of the protected matter must be made as soon as the scene has been released by AU-40.

Open and Unattended Security Containers and Vault-Type Rooms:

If a security container or VTR is found open and unattended at any time, the individual making the discovery must notify the DOE HQ protective force, who must, in turn, follow the plan of action detailed in HQ protective force post orders. The protective force contacts an individual authorized access to the security container (i.e., an individual listed on the SF-700), and that individual is then responsible for notifying the cognizant HSO.

The person notified of the discovery can either:

- Respond to the scene to inventory the contents of the container and personally relock the container, or

- Authorize the protective force to relock the container. The person notified or some other individual responsible for the container must inventory the contents of the container no later than the next working day.

The HSO will initiate action to change the combination, which must be considered potentially compromised, as soon as possible during duty hours or after the start of the next workday, as applicable. However, for an XO-series combination lock, the combination need not be changed if all of the following criteria are met:

- There is no reasonable or probable suspicion that the contents of the container have been disturbed.

- The numbers in the combination have not otherwise been compromised or subjected to compromise via a written or verbal record or communication.

- The existing combination has been tested to ensure its operability. If the existing combination to an XO-series lock fails to open the lock, a compromise must be assumed, and AU-40 must be immediately informed via secure communication.

NOTE: The combination to other than an XO-series combination lock must be considered compromised and therefore must be changed.

Security container combinations (SF-700s) stored within a container that has been found open and unattended may have to be changed. All stored SF-700 combination envelopes must be examined for tampering. An expanded inquiry must be conducted for any SF-700 envelope that is open or shows signs of tampering, or for any security container combination that is exposed by any means. The inquiry process must assume that any security container whose combination has been exposed is compromised.

During the security inquiry, if there is reasonable suspicion that the contents of the container have been disturbed (e.g., missing documents, rearranged material, combination was changed, an XO series combination lock no longer opens on the assigned combination, missing SF-700s, or other suspicious indicators), the Inquiry Officer must notify AU-40 before taking any further action.

Originals of the security documents associated with the container that was found open and unattended become supporting documentation for the inquiry; therefore, replacement documentation must be generated, and the combination may need to be changed, as described above.

Controlling Access to Security Repositories:

Individuals requiring access to a security container or VTR must have a security clearance and special accesses for the highest classification level and most restrictive category, as

well as caveat requirements, of the information stored in that repository. For example, only individuals with a Q security clearance may have the combination for a container holding S/RD. Also, the container in this example would have to be secured if an individual with an L security clearance were to work in the same room with the container. Access to the combinations of security containers should be limited to a minimal number of cleared individuals.

Containers containing classified matter must be secured when an individual with the appropriate security clearance does not have visual line-of-sight to the front of the container.

Containers may not be left open and unattended when inside a locked room unless the room is authorized for open storage of the highest level and category stored in the open container.

A security container with a combination lock on each drawer (multilock security container) must have a separate classified combination for each drawer, each one with a separate SF-700. A multilocked cabinet is not considered secured unless all locks are locked with a classified combination (the 50-25-50 standard combination may not be used on unused drawers). Multi-lock containers are generally used for compartmentation purposes. If an SF-702 is used for each drawer, the combination lock on each drawer must be checked at the close of each business day.

A security container containing dual locks (two locks on each drawer), or an XO series lock used in the dual or supervisory combination mode (XO-series combination selection modes #2 and #3), normally referred to as "two-man control," must use an SF-700 for each combination lock, or single XO series lock with dual combination control enabled. The SF-700s for all such combinations must be stored in separate containers unless programmatic requirements dictate otherwise.

Most classified documents may be commingled within the same file folder; however, security clearance and need-to-know must be taken into consideration when filing classified documents. Classified documents removed from security containers must have the appropriate cover sheet attached. File folders containing classified matter, when removed from security containers, must be marked top and bottom, front and back, with the highest classification level of the contents or, alternatively, must have an appropriate cover sheet(s) attached.

Storage Requirements for NATO and DOS Documents:

North Atlantic Treaty Organization (NATO) documents must be segregated from other documents when stored in security containers. At a minimum, NATO documents may be segregated by being placed in separate files. Access to NATO documents requires an access briefing administered by the NNSA Security Operations Division (NA-71), which performs NATO Sub-registry functions for HQ. If NATO documents are stored in a

container with other classified documents, access to the container itself must be limited only to those individuals who have been granted access to NATO information. The record copy of the combination to a security container storing NATO information must be appropriately stored in another container authorized for the storage of NATO information.

U.S. State Department documents with the protective marking NODIS (No Distribution) are controlled by the Office of the Executive Secretariat, which also controls access to these documents. Document storage is limited to Office of the Executive Secretariat's LAs or VTRs and other organizations so designated by the Office of the Executive Secretariat.

End-Of-Day Security Check:

An SF-701, *Activity Security Checklist* (or equivalent form) must be used for end-of-day security checks of LAs and VTRs that contain security interests (e.g., security repository, classified computer, classified shredder). These forms should be maintained **inside** each LA or VTR. The form must be retained for 90 days following the date of the last entry unless involved in a security incident, in which case the form relevant to the inquiry is retained as an attachment to the Security Incident Report.

Open Storage Requirements:

Open storage of classified matter up to and including TS/RD may be authorized within rooms that meet VTR requirements, including alarm protection and XO-series combination locks on the door. Open storage approvals and certificates must be granted by AU-40 before open storage is implemented (see Chapter 2 (HQFMSP), Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs).

Individuals who access these areas must possess a security clearance for the highest classification level and most restrictive category of information that is in open storage. Individuals without the appropriate security clearance or need-to-know must be escorted by a person with the appropriate security clearance and need-to-know while they are in the area. The escort must ensure that the escorted individual is not given access to information that the individual is not authorized to access.

All classified matter exceeding the clearance level of the person to be escorted, including such items as classified equipment and/or classified maps, photographs, and charts on walls, must be covered or removed from the view of any individual requiring escort before that person (with escort) enters.

All individuals who are not assigned to, who do not work in, or who are not listed on the area access list posted within the open storage VTR must sign in on a visitor log, which contains a printed name, signature, date, time in, time out, and name of escort. Visitor logs for these approved areas must be retained for five years. Visitor logs may be locally produced.

Access control, whether by mechanical means, electromechanical means, or personnel, must be strictly maintained. An open storage LA or VTR may never be left unoccupied unless fully locked with the XO-series combination lock and alarmed.

Security Container Check Sheet:

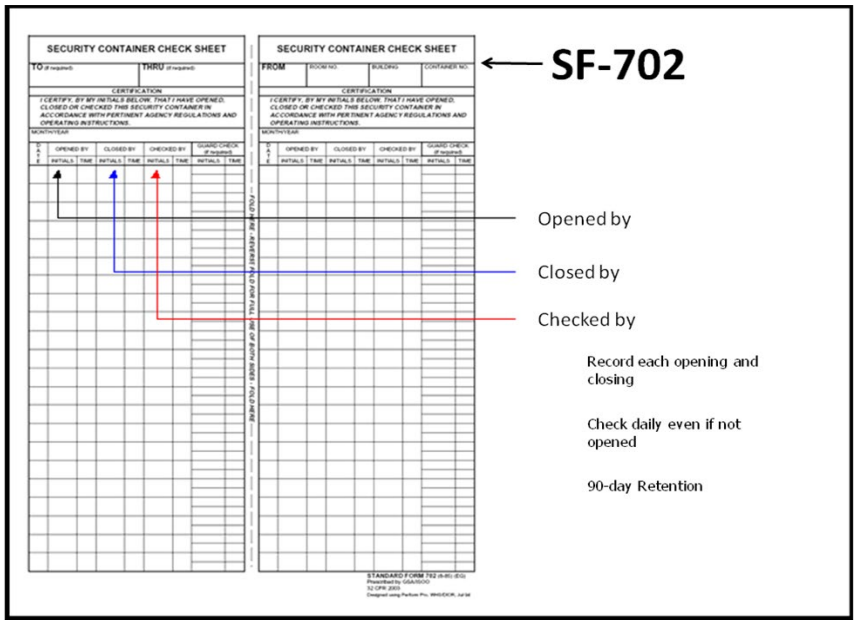
An SF-702, *Security Container Check Sheet* (document linked at end of section in Forms/Samples/Graphics), must be placed on each security container; on each combination-locked access door to a security area authorized for open storage of classified matter; and on each VTR entrance on the outside of the locking door so as to ensure high visibility upon inspection.

The SF-702 must be completed by the individual who opens, closes, or checks the security container, combination-locked security area access door, or VTR. In all cases, the individual who opens a security container is responsible for closing the container or transferring the responsibility for the security of that container to another authorized individual.

An SF-702 must contain at least one daily duty-day entry that the container was "checked by" with time and initials, regardless of whether the container was opened that day. Protective force checks, when required, are in addition to this check. Each container opening and closing must be recorded throughout the day except when the container is used by a sole custodian, in which case only one opening and closing entry is required. Another individual should annotate the "checked by" box, but if no one else is available, the person closing the container may fill in the "checked by." The SF 702s are expected to be completed each day there is activity in the work area. Each office/work space is encouraged to develop a process to ensure that all classified matter is properly stored and that security containers are checked at the end of each work day.

SF-702s must be retained for 90 days after the last date of entry on the form.

NOTE : Security containers located within approved open storage areas may or may not require the use of a separate SF-702, depending on the nature of the classified matter stored therein. Contact the CMPC Program Manager, AU-42, for guidance.



Security Repository (Safes and Doors) Combination Information:

Combinations to security containers, authorized open storage area combination-locked security access doors, and VTRs must be changed by an appropriately cleared individual who has authorized access to the combination. A change of combination and creation of a new SF-700, *Security Container Information*, is required when:

- An employee with access to the repository leaves, no longer requires access, or is no longer permitted access (includes administrative termination, suspension, or downgrading of security clearance lower than the level of classified matter being stored).
- There has been a known compromise, possible compromise, or discovery of a security repository that was left unlocked/open and unattended.
- The repository is put into service.
- The repository is taken out of service or prepared for turn-in; see Moving Security Containers (Safes), below.
- Maintenance has been performed on the repository by anyone other than individuals with required access, regardless of whether or not the lock was accessed or serviced. XO-series locks, combinations for which were NOT provided to a maintenance technician, are exempt from combination changing IF the locking device portion of the container was not removed from the LA or VTR for servicing, AND the XO combination was tested to ensure the validity of the combination in place prior to

servicing. If the known or existing combination does not function, this finding must be handled as a security incident and reported via secure channels.

NOTE 1: Combinations to containers storing NATO classified information must be changed at least annually. Combinations to containers storing communications security material must be changed every 2 years.

NOTE 2: The name and signature of the cleared individual changing a combination must be indicated in the "changed by" signature block of the SF-700.

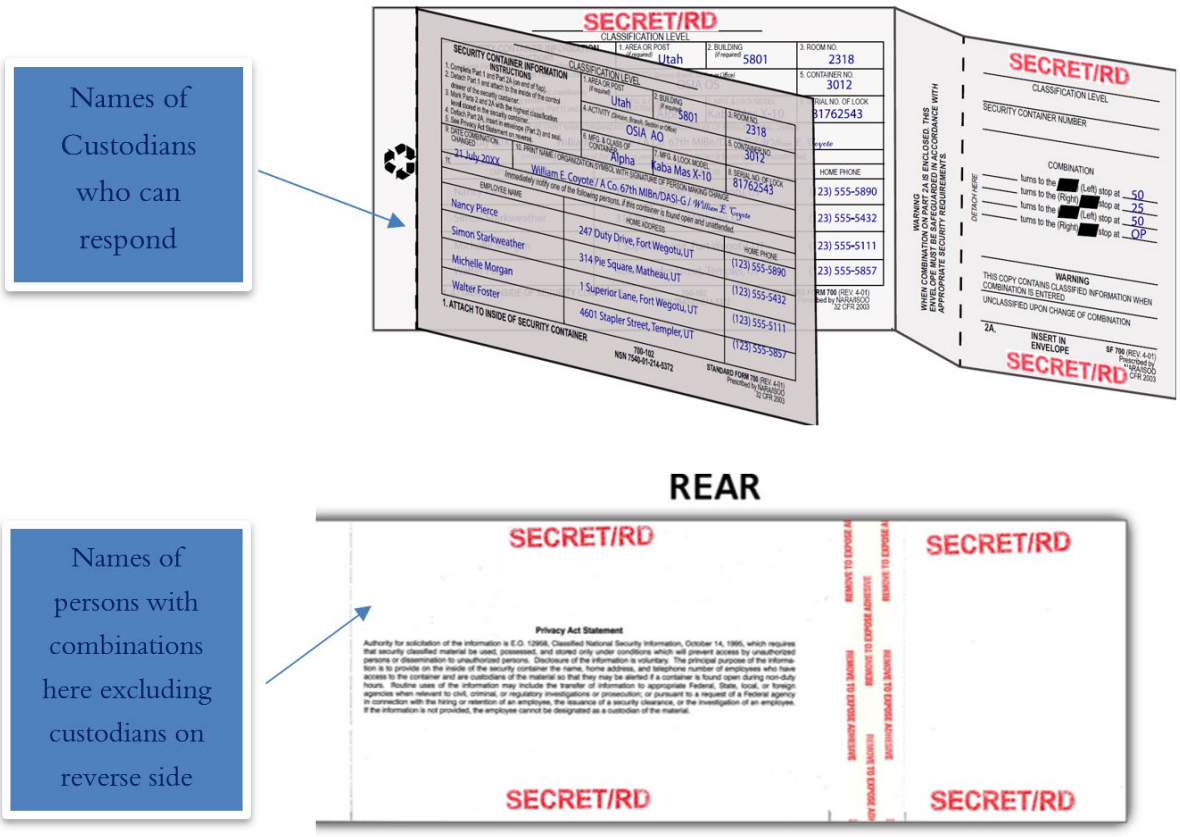
*NOTE 3: The requested XO-series lock serial number information in block 8 of the April 2001 version of the SF-700 is **NOT** required at HQ. The risk of lockout and damage to the XO-series lock outweighs any gained advantage of extracting the serial number.*

NOTE 4: Top Secret combinations must be brought into accountability.

NOTE 5: Combinations to containers storing accountable NATO classified information must be brought into accountability by the appointed document control officer of the approved NATO registry element.

The SF-700 is used to record the following important information about each security container:

- The location of the container
- The date and other pertinent information concerning the last combination change
- The names of the individuals who know the combination to the container
- The name, address, and phone number of custodians who can respond should the container be found open and unattended
- The combination to the container



The cover sheet (Part 1) of the SF-700 is to be completed, detached from the envelope portion of the form (Parts 2 and 2A), and affixed inside each lockable drawer of a security container or on the inside of the door to a VTR. The cover sheet (Part 1) is not to be affixed to the outside/exposed portion of a container or door and should not have any classification markings on it. The cover sheet should include:

- The room number and building where the container is located
- The date of the last combination change and the name and office symbol of the person who changed the combination
- The name, home address, and phone number of custodians who can respond if the container is found open and unattended
- Other repository custodians, without emergency responsibilities, must also be listed, but addresses and phone numbers are not required. Additional cleared personnel are added to this record when they receive the combination.

NOTE: There must be no external indication on any container or door as to the level of classified matter contained therein.

SUGGESTION: The record of non-emergency custodians may be maintained on the back side of the SF-700 envelope, or on a separate paper or card attached to the SF-700. Any other readily recallable record is also acceptable.

Part 2A of the SF-700 should be detached from the envelope portion of the form (Part 2) and the combination to the container entered onto it. Part 2A must then be marked on both the top and bottom of the front and back with the highest classification level and category of information stored in the container and sealed inside the envelope (Part 2). The envelope must be marked top and bottom, front and back, with the highest classification **level and category** of the information authorized to be stored in the security container. Classification authority or declassification instructions are not required on any portion of the SF-700.

NOTE 1: Combinations are classified and should be committed to memory. Due to the vulnerability of the sealed flap on Part 2 of SF-700, it is suggested that brown paper sealing tape be placed over the flap and that a signature be affixed to the tape intersection with the envelope. Container combinations recorded on Part 2A, enclosed in Part 2 of SF-700, are to be stored in a centralized repository authorized for an equal or higher classification level and category. HSOs should determine the storage locations for such SF-700s by element or sub-element. Combinations protecting SCI must be stored within a SCIF. An SF-700 containing a TS combination must be appropriately stored and brought into accountability. The creation of a "master combination list" of multiple combinations for any program, office, or element is ***prohibited****.*

NOTE 2: A record copy of combinations to VTRs and LAs, contained in properly marked, individually sealed envelopes, should be provided to the local CAS for storage. For purposes of life safety and emergency response, the CAS ensures that the HQ protective force has access to those combinations and/or keys to locking devices that deny ready access to occupied areas.

Superseded SF-700s should be destroyed as classified matter as soon as they are replaced.

Moving Security Containers (Safes):

HSOs must become involved in the relocation or turn-in of a security container so they can ensure that appropriate security precautions are taken and can then properly annotate their security container records. There are three possible reasons for moving a safe:

1. <u>The safe is no longer needed and will be turned in as excess</u> – In this case, the HSO coordinates with the element's Accountable Property Representative (APR), and the Office of Management (MA) to ensure that the safe is empty, the combination is reset, and the movement is completed. The HSO is responsible for removing the safe from his/her Appendix to the HQFMSP. Detailed instructions for HSOs in turning in

a safe are included in the 'How to Excess a Safe' document (located on the Chapter 5 download page).

2. The safe is being relocated to another room with no change in custodians – In this case, the HSO coordinates with the element's APR and MA to ensure that the safe is configured for movement and that the movement is completed. The HSO is responsible for updating his/her Appendix to the HQFMSP to show the new location of the safe. Detailed instructions for HSOs in relocating a safe with no change in custodians are included in the 'Moving a Safe with No Change in Custodian' document (located on the Chapter 5 download page).

3. The safe is being transferred to another custodian – In this case, the HSO coordinates with the element's APR and MA to ensure that the safe is configured for movement and that the movement is completed. The HSO is responsible for updating his/her Appendix to the HQFMSP to show the new location and/or custodian of the safe. Detailed instructions for HSOs in relocating a safe with a change in custodians are included in the 'Moving a Safe with a Change in Custodian' document (located on the Chapter 5 download page).

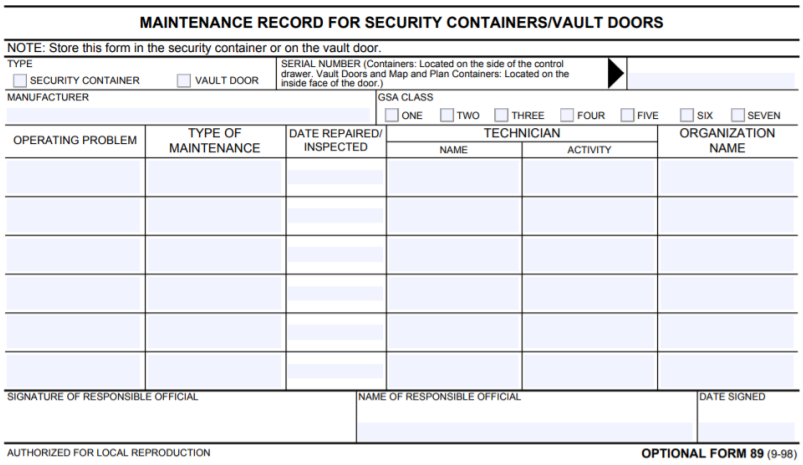
NOTE: Relocating a security container and/or rearranging furniture within an alarmed room may interfere with the electronic protective system. Therefore, contact the Office of Physical Protection, (AU-41). Who may require that a security system performance test be conducted immediately after the move.

Use of Optional Form 89, *Maintenance Record for Security Containers/Vault Doors*:

An *Optional Form 89, Maintenance Record for Security Containers* must be placed inside the control drawer of each security container and posted on the back of a door with a combination lock installed on it. The servicing lock or container technician uses the OF 89 whenever the security container is serviced or repaired. This form must remain inside the drawer or on the back of the door for the life of the container. **Do not remove the form when excessing the container.**

If a container has been drilled or otherwise modified to gain entry, a statement of repair must be entered and signed on the OF 89 by the technician and/or inspector, stating that the repair was in accordance with GSA standards (Federal Standard 809A), before the container can return to use for storage of classified matter. Alternatively, the certification statement may be attached to OF 89. If a security container has not been restored to GSA standards, the GSA certification label on the front of the container must be removed and a permanent sign affixed to the front stating "Not Authorized for Classified Storage."

Optional Form (OF)-89



MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS

NOTE: Store this form in the security container or on the vault door.

TYPE ☐ SECURITY CONTAINER ☐ VAULT DOOR

SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Map and Plan Containers: Located on the inside face of the door.)

MANUFACTURER

GSA CLASS ☐ ONE ☐ TWO ☐ THREE ☐ FOUR ☐ FIVE ☐ SIX ☐ SEVEN

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION **OPTIONAL FORM 89** (9-98)

24-Hour Classified Receipt and Storage:

Any person who has possession of classified matter up to TS/RD (not including SCI and SAP matter) and cannot store it in a classified repository (e.g., lock failure, don't have the combination to the safe, after-hours courier, etc.) can deliver the matter to the Forrestal or Germantown CAS for storage. The CASs are available 24 hours a day, every day, for classified receipt and storage:

- The Forrestal CAS is located in Room 1G-022.
- The Germantown CAS is located in Room A-060.

The person in possession of the classified matter must leave it in its classified wrapper and deliver it to the CAS. CAS operators will provide a receipt for the classified package(s) and provide temporary storage until the next normal business day. The person who retrieves the stored classified matter from the CAS must present the signed receipt and appropriate DOE identification.

NOTE 1: Temporary storage of SCI or SAP material should be arranged separately, in advance, if possible, with the program office concerned.

*NOTE 2: **Temporary After-Hours SCI Storage (Forrestal Only)** – On normal business days from 7 a.m. until 8 p.m., SCI material may be taken to and stored in the Forrestal DOE/IN Communications Center (GA-293). The phone number is (202) 586-8686. This phone number is also monitored by the IN Communications Center duty officer when the Communications Center is closed. When notified by telephone that a request has been made for SCI material to be stored after normal business hours, the duty officer arranges for appropriately cleared IN personnel to meet with the requester in the Forrestal building to accept*

the SCI material and store it in accordance with programmatic requirements.

NOTE 3: ***Temporary After-Hours SAP Storage*** *– After-hours storage of SAP material must be initiated by the requester at the* ***Forrestal CAS*** *located in room 1G-022. Upon notification by the requester, the CAS Operator will notify designated SAP personnel. In response to the notification, SAP personnel will respond to the Forrestal CAS to take possession of the material and store it in accordance with programmatic requirements.*

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (202) 586-4487 or contact the Office of Information Security

The following forms and graphics are available on the Chapter 5 download page:

How to Excess a Safe

Moving a Safe with No Change in Custodian

Moving a Safe with a Change in Custodian

Sample Not Authorized for Classified Destruction Sign

Forms/Samples/Graphics

OF 89, *Maintenance Record for Security Containers/Vault Doors Federal Standard* (for a copy of this form go to Optional Form, Maintenance Record for Security Containers/Vault Doors)

SF-700, *Security Container Information* (to order this form go to Standard Form-700, Security Container Information). Originals of this form can be obtained from the Forrestal and Germantown Supply Centers.

SF-701, *Activity Security Checklist* (for a copy of this form go to Standard Form-701, Activity Security Checklist)

SF-702, *Security Container Checksheet,* (for a copy of this form go to Standard Form-702, Security Container Checksheet)

HQ F 5632.12, *Container Equipment Inspection Certificate* (this form is available from the Forrestal and Germantown Copy Centers)

Helpful Websites

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

Section 508
Reproducing Classified Matter

This section describes how to properly reproduce classified documents at DOE HQ.

HQ Implementation Procedures

Reproduction of classified documents must be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations indicated on the document. Reproduction must be performed by authorized, appropriately cleared individuals knowledgeable of the procedures for classified reproduction and only in the performance of official or contractual duties. Reproduced copies are subject to the same protection and control requirements as the original.

Restrictions:

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. Markings that limit the reproduction of classified matter include:

- TS/FGI may not be reproduced without the express permission of the originating government, except as needed to facilitate review for declassification. However, after such reviews are completed, reproduced documents containing classified information must be destroyed in accordance with Section 514, Destruction of Classified Matter.

- For Intelligence Community documents only, the Originator Controlled (ORCON) caveat marking may be used to restrict reproduction to only that allowed by the originator.

- For non-Intelligence Community documents, the following statement, or one similar in content, may be used to restrict reproduction to that allowed by the originator:

REPRODUCTION REQUIRES APPROVAL OF THE ORIGINATOR

Reproduced accountable documents must be brought into accountability (see Section 509, Accountability of Classified Matter).

Reproduction Machines:

Reproduction of classified documents in HQ facilities must be accomplished only on machines located within LAs or VTRs that are specifically approved for classified reproduction. The LA or VTR must also be accredited for classified reproduction and be so annotated on the Security

Area Approval certificate (see Chapter 2, Limited Areas and Vault-Type Rooms). Machines approved for classified reproduction are designated by conspicuously posted copier certification signs specifying the highest level and category of classified matter that may be reproduced. The copier certification sign must contain the make, model and DOE property number of the authorized copier and be signed and dated by the element HSO and/or Information Systems Security Manager (ISSM). Certification signs for classified reproduction machines are machine - and room specific. Relocation or replacement of a classified copier requires a newly initiated sign. A sample of the Certification Sign is provided on the Chapter 5 download page. Additionally, notices regarding any restrictions or requirements pertaining to the reproduction of classified documents on a particular copier must also be posted conspicuously next to the copier. A sample of Classified Reproduction Procedural Instructions to be posted by the HSO is provided in Sample 508-1.

All Headquarters reproduction machines that are within an LA or VTR but are NOT approved for classified reproduction must have a sign posted near the machine indicating it is not approved for classified reproduction. A sample sign is provided in Sample 508-2.

NOTE: All facsimile machines are considered to be copiers and are subject to the same signage requirements as copiers.

NOTE: Printers have the ability to produce copies and are also subject to the same signage requirements as copiers.

Both classified and unclassified digital copiers must undergo an approval process prior to purchase or lease. The element ISSM can help determine which digital copiers may be acquired and what security measures must be met. Also, the element HSO should be informed when a new copier is acquired.

NOTE: Any printer, copier or multi-function device used for classified processing must

- *Be covered by an approved Classified System Security Plan*
- *Have had a Supply Chain Management Review (SCRM) decision by the cognizant AO*
- *Must have a National Information Assurance Partnership (NIAP) Approved Protection Profile (or equivalent).*

Any printer, copier or multi-function device, standalone or networked that is located inside of an LA or VTR that is only accredited for closed storage and for classified reproduction at the confidential or secret level is authorized to have its factory storage (i.e. hard drive, on board writable flash storage, etc.) remain in-tact as long the following conditions are met and measures are taken by the owning office elements cyber security accrediting authority's team (i.e. ISSO, ISSM and AO) which will demonstrate acceptable positive control with-in the LA or VTR that is only accredited for closed storage.

- Storage device must at a minimum must be encrypted at AES-256 at rest

- A technical review must be performed on the make and model by DOE Office of Technical Security (AU-1.22) Technical Security Program (TSP) on at least 25% of the same lot that was procured
- DOE approved prismatic seals must be used on any key areas of the storage device where it could be removed
- The seals must be tracked by serial number by the owning origination cyber security element and report any sign of tampering to the organizations HSO and ISSM. The seals must be checked by the owning organizations cyber security element bi-annually and report the status to the ISSM.

Reproduction Process:

Inside an LA or VTR, classified documents must be transported to and from the reproduction machine area in the appropriate manner (see Section 511, Receipt and Transmission of Classified Matter). Access to classified matter being reproduced must be controlled to preclude unauthorized disclosure.

When copying is complete, the reproduction path and all paper trays of the reproduction machine should be checked to ensure no classified matter has been retained. Collection trays of double-sided copy machines demand particular attention. Any remaining classified matter should be handled and disposed of in a manner approved for classified destruction.

After reproduction has been completed, one blank copy should be made and carefully examined to ensure that all residual images are eliminated from the machine. If examination of this blank copy reveals no images, it may be disposed of normally (recycle or general trash, as appropriate). If any previously reproduced image or portion thereof appears on the blank copy, repeat the procedure as necessary, handling and disposing of all blank copies as classified non-accountable matter. Contact your HSO immediately regarding this problem.

If a paper jam or other malfunction cannot be readily resolved, the HSO must be summoned; however, at no time may classified matter be left unattended within the copier room or area. The phone number of the HSO is posted on the certificate for the classified copier. A passerby may be summoned to provide assistance in contacting the HSO.

Classified copies should be properly marked as soon as possible.

Reproducing classified matter on copiers located outside of LAs and VTRs is PROHIBITED.

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (301) 903-9990 or (202) 586-4487

The following forms and graphics are available on the Chapter 5 download page:

Sample Classified Reproduction Certification Sign

Forms/Samples/Graphics

Sample Classified Reproduction Procedural Instructions Sign (see Sample 508-1)

Sample Copier Not Approved for Classified Sign (see Sample 508-2)

SAMPLE 508-1

Sample Classified Reproduction Procedural Instructions

CLASSIFIED REPRODUCTION PROCEDURAL INSTRUCTIONS FOR DIGITAL COPIERS

1. See accompanying *AUTHORIZATION SIGN* for classification limits and instructions.
2. Observation of classified operations must be limited to person with appropriate clearance and need to know.
3. Reproduction authorizations are required for ORCON, NATO, SCI, or other control caveats which limit or prohibit reproduction without special permission.
4. Limit number of copies to only that which is absolutely required. If matter is accountable, all copies must be brought under control.
5. Unacceptable or excess copies MUST be collected and destroyed as classified information (accountability and destruction receipts not required).
6. After copying operations are completed, see "Sanitization Procedures for Digital Copies" sign for sanitization instructions.
7. DOUBLE CHECK the copying area before departing to ensure no classified matter remains (i.e., originals removed from copying plate, copies removed from machine collection tray(s) or collating bin(s), and copies to be destroyed are collected).
8. The ISSM/HSO must be notified of any anomalies experienced during the classified copying process (i.e., paper jams, images remaining on the blank copy, unauthorized exposure of uncleared individuals to classified information, classified documents found in the copier at the start of copying operation, etc.)

POST THIS NOTICE IN THE IMMEDIATE VICINITY OF COPIERS USED FOR CLASSFIED REPRODUCTION

SAMPLE 508-2

Sample Copier Not Approved for Classified Sign

Section 509
Accountability of Classified Matter

Most classified matter does not require accountability; however, several types of classified matter do require accountability due to national, international, or programmatic requirements. Accountability systems provide an audit trail or chain of custody for the Department's most sensitive classified documents and media. Types of classified matter encountered at DOE HQ that require accountability include, but may not be limited to:

- All TS matter, including TS/FGI
- S/RD (or higher) matter stored outside an LA or higher
- Any matter that requires accountability because of national, international, or programmatic requirements
- National requirements, such as Cryptography (CRYPTO) and designated COMSEC
- International requirements, such as NATO ATOMAL (Restricted Data), designated United Kingdom (UK) documents, or other FGI designated in international agreements
- Special programmatic requirements (e.g., SAP and Sigma 14)
- Secret documents containing FGI if so, designated in a treaty or international agreement
- Prior to April 12, 2011, media containing S/RD or higher was designated as Accountable Classified Removable Electronic Media (ACREM) and was accountable. After April 12, 2011, media formerly designated as ACREM remains accountable only if it qualifies under the current definition of accountable matter contained in DOE Order 471.6, *Information Security*. The media formerly designated as ACREM must remain in accountability until verification that none of the information that requires the media to be accountable (including nuclear weapons data) can be retrieved or recovered from that piece of media, or until the media is destroyed. The term ACREM is no longer used.
- Completed Parts 2 and 2A of SF-700, *Security Container Information*, constitute an accountable document if any of the information stored in that container is accountable. It does not, however, need to be placed into the formal accountability system (as detailed below). A simple paper or computerized log will satisfy accountability requirements for these parts of the SF-700 if the log includes the container number as the unique identification number, date created, classification level and category, and date taken out of accountability and reason (e.g., change of combination, or turn-in of container). Classifier and declassification information are not required on an SF-700.

HQ Implementation Procedures

Accountability Systems:

Classified Document Control Station (CDCS) personnel within each HQ element, with the assistance of the HQ CMPC Program Manager, must establish a system to track the element's accountable classified matter. See Section 510, Classified Document Control Stations, for a discussion of CDCS operations. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, or changed in classification. Accountable documents must be assigned a unique number to track the document throughout its life in that office. The accountability system must have the capability to reflect each transaction (generation, reproduction, transmission, declassification/downgrading, destruction, etc.) performed for documents entered into the accountability system. Overall accountability system requirements are detailed in DOE Order 471.6, *Information Security*.

Inventories:

CDCS personnel must inventory all accountable documents annually. The inventory must include a visual verification of each document, as well as a reconciliation of the documents on hand with the list of documents in the accountability records.

Any discrepancies found during the inventory must be reported to the element HSO, who must in turn report those findings to the HQ Security Incidents Program Manager within AU-41 and the CMPC Program Manager within AU-42. Inventory discrepancies may be reportable as Incidents of Security Concern as described in Chapter 11, Incidents of Security Concern. The HQ Security Incidents Program Manager may instruct the element HSO to complete and submit DOE F 5639.2 | Department of Energy, *Reporting Unaccounted for Documents* in order to document the inventory discrepancy.

In conjunction with the inventory process, or on a continuous basis, HSOs are to ensure that organizational classified holdings are reviewed for the purpose of inventory reduction.

Accountability Records:

Accountability records must include the following information for each accountable item:

- Date of the matter
- Brief description of the matter (unclassified description preferred)
- Unique identification number (each document, including reproductions, must have a unique number assigned to it)
- Classification level, category (if RD/FRD/TFNI), and caveat (if any)

- Disposition of the accountable matter (e.g., destruction, reproduction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record and the date)
- Originator identification
- Authority for contractor retention
- Date received (if applicable)
- Office/activity from which the matter was received (if applicable), including the office or activity name and address from which matter was transmitted to the recipient
- The individual who checked it in and/or out (i.e., the person who has personal responsibility for it and date).

Accountability records ensure a chain of custody so that all accountable matter can be located at any given time, whether it is stored or in use. Accountability procedures should be recorded in an organization's CDCS procedures (see Section 510, Classified Document Control Stations).

Accountable information temporarily transferred to another organization within the same facility must be entered into the receiving organization's accountability records if the material is kept more than 180 days without return to the sender.

Master files and databases created in central data-processing facilities to supplement or replace Top Secret records are not authorized for disposal under General Records Schedule 18. This type of file must be scheduled on DOE F 1324.5, *Request for Records Disposition Authority*.

All accountability records (e.g., logs, inventory records, receipts) for Secret and Confidential material shall be maintained for two years. Accountability records for Top Secret shall be maintained for five years.

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (301) 903-9990 or 202-586-4487.

Forms/Samples/Graphics

DOE Form 5639.2, *Reporting Unaccounted for Documents* (for a copy of this form go to DOE Form 5639.2, Reporting Unaccounted for Documents)

DOE F 1324.5, *Request for Records Disposition Authority* (for a copy of this form go to *DOE Form 1324.5, Request for Records Disposition Authority*)

Helpful Websites

To view DOE Order 471.6, *Information Security*, go to: DOE Order 471.6 Admin Chg 3, Information Security.

Section 510
Classified Document Control Stations

DOE Order 471.6, *Information Security*, requires that control stations be established to control the classified matter received by and/or dispatched from DOE facilities. Personnel must be designated and specially trained to operate these control stations and must have security clearances commensurate with the level of their classified matter control responsibilities. At DOE HQ, a control station is known as a Classified Document Control Station (CDCS).

HQ Implementation Procedures

Applicability and Scope:

Each HQ element that receives or transmits classified matter, or that has the potential to receive or transmit classified matter, must establish at least one CDCS. A CDCS is a gateway through which all incoming and outgoing classified matter must transit. HQ elements may establish more than one CDCS, such as one at the Forrestal Building and another at the Germantown Building, when additional CDCSs are needed for efficient operations. An HQ element that has minimal classified holdings or only an occasional need to receive or transmit classified matter may establish a partnership with another element to use their CDCS.

The purpose of the CDCS is to prevent unauthorized access to and unauthorized removal of the element's classified matter. A CDCS is the primary point where classified matter may be received or transmitted by the HQ element. CDCS personnel generate the records required for the receipt and transmittal of classified matter, maintain access lists (when required), and generally control the classified matter received by and/or dispatched from the element.

CDCS Standard Operating Procedures must be developed in detail and updated as necessary by the station operators in consultation with the element HSO and the HQ CMPC Program Manager.

Appointments and Designations:

1. CDC Station Operators and Alternates – The Head of each HQ element with a CDCS, **or his/her designee**, must appoint one Primary CDCS Operator and at least one Alternate CDCS Operator for each CDCS within the element. The responsible HSO must enter the names of the appointees into the element's Appendix to the HQFMSP and must notify the CMPC Program Manager in writing. The names of the appointees must be readily available for surveys and inspections. The number of CDCS operators should be kept to the minimum required to process the amount of classified mail, facsimiles, and other matter received or transmitted by the element.

CDCS personnel must possess a security clearance commensurate with the highest level and category of classified matter that passes through the CDCS.

2. Classified Mailing Address (CMA) Authorized Designees – Each HQ element with a CDCS must appoint specific cleared individuals to act as CMA Authorized Designees, who are authorized to receive classified United States Postal Service (USPS) mail from the Forrestal and Germantown Central Mailrooms. CMA Authorized Designees are normally the CDCS operators; however, in unique circumstances where minimal additional designees are required, other cleared personnel may be appointed. CMA Authorized Designees who are not CDCS operators must be trained by their HSO or the HQ CMPC Program Manager in the handling of classified matter in accordance with operational procedures in place within the organization.

   Since the Central Mailrooms at the Forrestal and Germantown Buildings will only deliver classified mail to a CDCS, they need to be informed of the locations of all CDCSs and the names of the CMA Authorized Designees who can accept classified mail when it is delivered. The mailrooms obtain this information from the registry of CDCSs and CMA Authorized Designees that is maintained by the HQ CMPC Program Manager.

   HSOs must send an e-mail to the Office of Information Security identifying the locations of their element's CDCS(s) and the names of their CMA Authorized Designees and verify and provide the current clearance level for those individuals. The HSO must also provide immediate e-mail updates as required. Refer to Attachment 510-1 for a sample of the email template. The HQ CMPC Program Manager uses the e-mails to maintain the registry of CDCSs and designees.

   The HSO must also provide immediate e-mail updates as required. Refer to Attachment 510-1for a sample of the email template. The HQ CMPC Program Manager uses the e-mails to maintain the registry of CDCSs and designees.

3. Express Mail Document Control (EMDC) Designees – All incoming overnight express mail has the potential to contain classified matter; therefore, all overnight express mail packages must be handled as classified matter. Each HQ element with a CDCS must appoint specific, cleared individuals to act as EMDC Designees.

   HSOs must send an e-mail identifying the names of their EMDC Designees and must provide immediate e-mail updates whenever there are changes. The e-mail address to be used for the updates is shown in Attachment 510-2. The HQ CMPC Program Manager uses these e-mails to maintain a registry of EMDCs.

Training:

All CDCS personnel must complete CDCS training before assuming CDCS duties. This training is tailored to the responsibilities of CDCS personnel and includes the following

subject areas: generation and marking, physical protection and storage, reproduction, accountability, transmission, and receipting (including hand-carry), destruction, and emergency procedures. CDCS training is provided by the HQ CMPC Program Manager. On a case-by-case basis, the CMPC Program Manager is authorized to temporarily waive the training requirement based on an individual's previous experience and the ability of the organization's HSO to guide the individual on CDCS duties until the formal training is available.

CDCS Operations:

1. Receipt of Classified Matter – All incoming classified matter must transit through an element's CDCS before being released for storage in any other organization's designated classified document repository. This requirement applies to all incoming classified mail, as well as other classified matter hand carried into HQ facilities.

   Upon receipt of the matter, CDCS personnel examine the package for evidence of tampering, as applicable, open the package, and determine whether to retain the material (e.g., accountable matter) or release it to another classified document repository custodian. When transferring classified matter to another authorized classified document repository custodian or classified matter user within the organization, CDCS personnel are responsible for ensuring that they give the classified matter only to individuals with appropriate security clearances (i.e., a security clearance equal to or higher than the information) and that the transfer is accomplished without compromising the material (e.g., left unattended on the desk of a repository custodian).

   CDCS personnel must inspect package contents to ensure all classified documents are marked with the highest classification level at the top and bottom of the front page and back page. CDCS personnel affix the appropriate classified cover sheet to the document (if it is not already affixed). For any other discrepancy in document marking, the document recipient is responsible for reconciling it with the sender.

   CDCS personnel are also responsible for reconciling the package contents with the document receipt and returning the signed receipt to the sender as soon as possible. Discrepancies between the package contents and the package receipt are reported immediately to the sender. If the discrepancy cannot be resolved in one business day, the HQ CMPC Program Manager must be notified. Copies of signed receipts are maintained at the CDCS in accordance with the DOE Records Schedule and the National Archives and Records Administration (NARA) General Records Schedule (2 years for Secret and Confidential, and 5 years for Top Secret).

   NOTE: Although receipts for Confidential matter are not required, any receipt received with Confidential matter must be signed and returned.

2. Transmission of Classified Matter – All classified matter being transmitted out of an HQ element (mailed or hand carried) must be processed through the element's

CDCS. CDCS personnel ensure that appropriate document receipts (such as DOE F 470.10, *Classified Matter Receipt)* are used, the package is properly marked and wrapped, and the appropriate mail carrier and CMAs are used. The document sender is responsible for ensuring that the document is properly marked with appropriate classification markings. Most organizations task the CDCS personnel with the responsibility for ensuring that the CMA has been verified by consulting the information contained in SSIMS. Additionally, it is the responsibility of the sender, not CDCS personnel, to provide the transmittal letter (when required) to be included in the package with the classified matter.

CDCS personnel prepare an outgoing *Classified Matter Receipt* in triplicate when mailing and quadruplicate when preparing a package for hand carry. They maintain a copy of the outgoing receipt in a suspense file until the signed receipt is returned from the recipient. Copies of returned signed receipts are maintained at the CDCS in accordance with the DOE Records Schedule and the NARA General Records Schedule (2 years for Secret and Confidential and 5 years for Top Secret).

NOTE 1: Classified Matter Receipts are not required for outgoing Confidential matter, unless the outgoing Confidential matter is being hand carried outside of an HQ facility and the receipt is used to document what matter is being hand carried.

NOTE 2: It is recommended that signed receipts be returned by the recipient within 15 days. Mandatory follow-up action is required if receipts are not returned within 30 days.

For all classified matter hand carried outside of an HQ facility, a copy of the receipt, or other manifest, must be left with the servicing CDCS, and one signed Unclassified copy must be carried on the person of the individual hand carrying the package. If the hand carried matter is returned to the same CDCS, the receipt copy is used to reconcile the original package contents with what is returned. If the hand carried matter is left at a destination and the courier had the recipient sign a receipt, the courier must return the receipt to the CDCS. If the hand carried matter is destroyed by the hand carrier at the destination, the individual should annotate the receipt with the date, time, and location of destruction; certify the destruction with his/her signature on the receipt; and return the receipt to the servicing CDCS, or certify the destruction using a DOE F 5635.9, *Record of Destruction*. The DOE F 5635.9 should be given to the appropriate CDCS personnel by the individual hand carrying the classified matter upon his/her return to the facility.

NOTE: Classified matter hand carried outside the facility but intended for return to the CDCS on the same day must be on record with the CDCS. All hand carried classified matter must be reconciled upon return to the facility.

Facsimile Classified Document Control Stations:

Since a facsimile machine is capable of receiving and transmitting information, a facsimile machine approved for receiving and transmitting classified documents is, by definition, a CDCS. A facsimile machine may function separately as a stand-alone CDCS, or it may be a piece of equipment within an established CDCS.

If the classified facsimile machine is a stand-alone CDCS, Primary and Alternate Control Station Operators must be appointed and listed in the element's Appendix to the HQFMSP in the same manner as a normal CDCS.

Although Primary and Alternate Control Station Operators are appointed for each classified facsimile machine, other users trained in the operation of the classified facsimile equipment and procedures may be authorized to use the equipment. Therefore, all classified facsimile machine users must comply with all the established procedures.

The person using the STE encryption interface to a classified facsimile machine is responsible for ensuring that the individual on the receiving end possesses the appropriate security clearance and need-to-know before transmitting any data. SSIMS validation is also required to ensure that the facility has the appropriate storage capability for the transmitted classified matter.

Receipt of classified facsimiles must be confirmed with the intended recipient. Facsimile logs, or separate receipts, must be retained for all (including Confidential) incoming and outgoing classified matter. NARA guidelines are applicable for maintaining records. Return facsimile receipts are preferable; however, verbal acknowledgement of receipt of classified transmission is permitted but must be annotated (either on the facsimile log or on the record copy of the outgoing facsimile cover page) with the name of the person receiving the classified facsimile, time and date received, and number of pages received. Discrepancies in the number of pages received and the number of pages transmitted must be resolved immediately.

Appropriate classification markings, as in any classified document, are required for all incoming and outgoing classified facsimiles. Specific attention must be given to the overall classification level marking of the outside of the back page of an incoming classified facsimile. If applicable, formal accountability for incoming and outgoing classified facsimiles is required.

Classified cover sheets must be applied to all incoming classified facsimiles immediately after receipt and before distribution.

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (202) 586-4487 or (301) 903-9990.

Forms/Samples/Graphics

Sample E-Mail Notification for Classified Mailing Address Authorized Designees (see Sample 510-1)

Sample E-Mail Notification for Express Mail Document Control Designees (see Sample 510-2)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to DOE Form 470.10, Classified Matter Receipt)

DOE F 5635.9, *Record of Destruction* (for a copy of this form go to DOE Form 5635.9, Record of Destruction)

Helpful Websites

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

SAMPLE 510-1

Sample E-Mail Notification for Classified Mailing Address Authorized Designees

Send the e-mail to: Office of Information Security

The e-mail "Subject" block should be: "Notification of Classified Mailing Address (CMA) Authorized Designees"

The body of e-mail should include the following information:

"The Office of _____ has approved the following personnel to receive and open classified USPS mail addressed to this office:
Name of Designee: Security Clearance Level: _____
Organization code and/or organizational name:
Building name Forrestal or Germantown:
Room number/location of Classified Document Control Station:
Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified USPS mail, and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO, Alternate HSO, or HSO Representative.

Information may appear in the following format (example):

FORRESTAL CMA REGISTRY						
Element	Organization	Point of Contact	Phone #	Room No.	Action	Clearance
AU	Office of Environment, Health, Safety and Security					
	AU-1.23	John DOE	202-586-xxxx	1A-123	ADD	Q
		Jane DOE	202-586-xxxx	1A-123	DELETE	Q

SAMPLE 510-2

Sample E-Mail Notification for Express Mail Document Control Designees

Send the e-mail to: Office of Information Security

The e-mail "Subject" block should be: "Notification of Express Mail Document Control Designees"

The body of e-mail should include the following information:

"The Office of _____ has approved the following personnel to receive and open express mail packages addressed to this office:
Name of Designee:_____Security Clearance Level: _____
Organization code and/or organizational name:
Building name (Forrestal or Germantown):
Room number/location of Classified Document Control Station:
Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified express mail, and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO Alternate HSO, or HSO Representative.

Information may appear in the following format (example):

FORRESTAL EXPRESS MAIL REGISTRY						
Element	Organization	Point of Contact	Phone #	Room No.	Action	Clearance
AU	Office of Environment, Health, Safety and Security					
	AU-1.23	John DOE	202-586-xxxx	1A-123	ADD	Q
		Jane DOE	202-586-xxxx	1A-123	DELETE	Q

Section 511
Receipt and Transmission of Classified Matter

This section describes DOE HQ procedures for the receipt and transmission of classified matter. The Forrestal, Germantown, and Portals facilities are the only HQ facilities authorized to conduct classified activities; therefore, classified matter can only be received or transmitted at those HQ facilities. DOE-approved contractor sites are permitted to receive and transmit classified matter in accordance with their DOE contract(s), their FDARs (DOE F 470.2 – see Chapter 4), and their security plans.

HQ Implementation Procedures

All classified matter received or transmitted by HQ elements must be processed through a CDCS (see Section 510, Classified Document Control Stations). The CDCS is responsible for receiving all classified matter addressed to the element and transmitting all classified matter dispatched by the element. In short, the element's CDCS is the organization's gateway for all incoming and outgoing classified matter. The CDCS also maintains the associated classified document receipts and any required inventory records.

Receiving Classified Matter by Mail:

All mail, including express mail, is initially received by the two HQ Central Mail Rooms located at the Forrestal and Germantown Buildings. The mailrooms sort and deliver the mail in accordance with established procedures. All registered, certified, and express mail is handled as controlled mail and distributed only to CDCS personnel who have been specifically designated to receive classified and express mail (see Section 512, Classified Mailing Addresses, and Section 513, Express Mail Service).

Receiving Classified Matter by Facsimile:

A classified facsimile machine is, in itself, a CDCS or part of an existing CDCS. Rules for receiving classified facsimiles are contained in Section 510, Classified Document Control Stations.

Headquarters Classified Mailing Addresses:

All classified mail being sent to a HQ element via the USPS must use the proper CMA.

The CMA for HQ elements located in the Forrestal and 955 L'Enfant Plaza facilities is:

ATTN: (ORGANIZATION) (INTENDED RECIPIENT)
U.S. DEPARTMENT OF ENERGY
P.O. BOX 23865
WASHINGTON, DC 20026-3865

The CMA for HQ elements located in the Germantown facility is:

ATTN: (ORGANIZATION) (INTENDED RECIPIENT)
U.S. DEPARTMENT OF ENERGY
P.O. BOX A
GERMANTOWN, MD 20875-0963

Transmitting Classified Matter in General:

Classified matter may be transmitted only in the performance of official and contractual duties. Unless the transmission is required by the specific terms of the contract or required for performance of the contract, the contractor must obtain written authorization from the contracting HQ element before transmitting classified matter outside of the facility.

The CDCS servicing an HQ element is expected to perform most of the actions associated with transmission of classified matter. These actions include selecting the proper method of transmission, packaging and wrapping the matter appropriately, preparing classified document receipts when required, maintaining transmission logs when required, and maintaining accountability records when required. The HQ CMPC Program Manager provides training for CDCS personnel throughout the year.

The individual for whom the CDCS is transmitting the classified matter is responsible for knowing the name of the intended recipient, verifying that he/she has the appropriate security clearance, and ensuring that he/she has need-to-know. **CDCS personnel are responsible for determining the recipient's CMA and verifying that the receiving facility is approved by DOE to store classified material at a classification level and category equal to or higher than what is being transmitted, unless the organization's CDCS procedures delegate that responsibility to some other individual(s).**

Transmission of Top Secret Matter:

Top Secret matter may be transmitted out of HQ facilities only by the Defense Courier Service, Department of State Courier System, approved communications networks (including approved classified facsimile), Headquarters Courier Service (within the Washington, D.C. metropolitan area), and designated hand carry personnel (as designated by the organizational hand carry approval authority). Use of the USPS or other commercial organizations is prohibited. The Washington, D.C. metropolitan area is defined as the area within a 50-mile radius of the Forrestal Building.

Approved Methods for Transmitting Secret and Confidential Matter Outside of a HQ Facility:

1. HQ Courier Service – The HQ Courier Service may be used to transmit Top Secret, Secret, and Confidential matter between the Forrestal and Germantown facilities and to other Federal agencies in the Washington, D.C. metropolitan area. Classified matter must

be **double wrapped**, properly marked, addressed to the proper CMA, and placed in an HQ F 1410.5, *Classified Matter between Offices in DOE Headquarters*, red and white ("Candy Stripe") envelope (see Sample 511-4). HQ F 1410.6, *DOE Messenger Receipt*, must be attached to the "Candy Stripe" envelope, and the transaction must be logged into the courier's register. All signatures on the HQ F 1410.6 must be accompanied by the signer's DOE badge number or printed name. Both the HQ F 1410.5 and the HQ F 1410.6 must include the recipient's name, organizational symbol, room number, and building or, if delivered to another government agency, the exact delivery point address. All classified matter to be couriered must also be accompanied by DOE F 470.10, *Classified Document Receipt*, or equivalent. These receipts must be retained for 5 years for Top Secret and 2 years for Secret and Confidential matter.

2. Transmission by the USPS – The USPS is the most common means of transmitting classified matter outside an HQ facility. All Confidential and Secret matter transmitted via USPS must be sent as Registered Mail, and the matter must be packaged and wrapped as described under "Packaging Classified Matter for Transmission Outside of an HQ Facility," below. The matter must be sent to a CMA that has been verified through SSIMS.

   USPS mail services cannot be used for Top Secret classified matter.

3. Transmission by Express Mail (Overnight Mail) Services – Express mail services shall not be used as a matter of routine or convenience for transmitting classified matter.

   Express mail services cannot be used for Top Secret classified matter.

   Use of any express service receptacles at or near a commercial building or at curbside locations is prohibited.

   At a minimum, the following conditions must be met concerning express mail:

   - Only designated CDCS personnel may prepare express mail packages for dispatch.

   - The HQ authorized commercial express mail service organization for outgoing classified express mail (overnight mail) is United Parcel Service (UPS). (Note: On rare occasions, a recipient organization may only accept incoming express mail service from a carrier other than UPS. The recipient's requirement to use a carrier other than UPS must be recorded in SSIMS.) OGAs may send express mail to DOE via other carriers.

   - Express mail addressees must be identified in SSIMS under "Overnight/Classified Common Carrier Address." (Note that this is always a street address.).

- The return address on DOE transmitted express mail is:

  - Forrestal: Sender's Name (Routing Symbol)
    U.S. Department of Energy
    1000 Independence Ave SW
    Washington, DC 20585

  - Germantown: Sender's Name (Routing Symbol)
    U.S. Department of Energy
    19901 Germantown Rd
    Germantown, MD 20874

Express mail must not be used to transmit classified matter on Fridays or on days preceding a holiday. "Next business day" deliveries on Fridays or the day before a holiday are not authorized.

All classified matter must be properly receipted, all packages must be double wrapped, and envelopes must be appropriately addressed before being inserted into the packaging provided by the express mail service.

There must be no mark on the external express mail box or envelope to indicate or imply that it contains classified matter. This restriction includes positional titles such as classified document custodian, security officer, classified control station, or any other wording that denotes or implies the presence of classified matter.

The sender must notify the intended recipient(s) of the proposed shipment and arrival date. There must be no reference to the fact that classified matter is being transmitted unless notification is made through a secure telephone. In addition, the sender must inform the addressee of the commercial carrier package Air Bill Label Number.

To ensure direct delivery to the addressee only, the release signature block on the Air Bill Label will not be executed under any circumstance.

4. Transmission by Facsimile – Only CDCS personnel or their designees/authorized users may operate classified facsimile machines. Transmission of classified information via facsimile machines that are not accredited for classified operation by the OCIO is strictly prohibited.

5. Hand Carry – Personnel with a security clearance equal to or higher than the classification level and category of classified matter to be transmitted may be authorized to hand carry it between destinations. The various circumstances involving hand carry are described in detail in the subsections below.

6. Transmission STE or vIPer – STE and vIPer devices must be used to transmit classified information telephonically. STEs and vIPers must be used within HQ LAs or VTRs unless the HQ Communications Security Program Manager within the Office of Corporate Security Strategy, Analysis and Special Operations (AU-1.2), has specifically

approved their use in other locations, such as the residences of senior DOE officials. Generally, the speakerphone capability of a STE or vIPer device will not be activated in the encrypted mode unless the LA or VTR has been approved for amplified discussion by the HQ Technical Security Program (TSP) Team.

a) Transmission by STE: Secure telephone calls are placed initially in the clear (non-secure) mode. When the caller desires to go secure, the keying device is activated by pressing the appropriate button on the instrument. This procedure places the instrument in the secure mode. The STE instrument then displays a message in the message window showing the highest classification level authorized to be discussed over the circuit. When not in use, the Fortezza card used to activate the STE's secure mode must be stored in a room separate from the STE instrument or in a GSA-approved repository in the same room as the STE instrument.

b) Transmission by vIPer: Secure telephone calls are placed initially in the clear (non-secure) mode. When the caller desires to go secure, the keying device is activated by pressing the unlock button and entering the user's PIN that is set when originally obtaining the vIPer. Once the call has been established, the user will then hit the secure button located on the phone. This procedure places the instrument in the secure mode. The vIPer instrument then displays a message in the message window showing the highest classification level authorized to be discussed over the circuit. When not in use, the vIPer will be placed in a locked state. The user's PIN will be considered classified and should not be shared with other individuals. If the PIN is written down on a document, it will need to be secured in a GSA approved safe.

The STE and vIPer user must clearly understand two important points:

- Users are responsible for ensuring that the individual on the distant end possesses the appropriate security clearance and need-to-know for the information being discussed.

- Users are responsible for ensuring that the classified portion of the discussion cannot be overheard by uncleared personnel who may be under escort inside or outside the local office area.

- Users are required to perform an electronic re-key call every six (6) months. The instructions to re-key are located on the STE or vIPer user agreements which are provided during initial install.

Also see Chapter 2, Limited Areas and Vault-Type Rooms (HQFMSP), Section 205, Secure Telecommunications Equipment (Phones).

Packaging Classified Matter for Transmission Outside of an HQ Facility:

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

1. Envelopes – When envelopes are used for packaging, the classified matter shall be protected from direct contact with the inner envelope. This can be done by affixing the appropriate cover sheet to both the front and back of the matter. The inner envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses, the overall classification level and category (if RD, FRD, or TFNI) 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 on the outer envelope indicating that the contents are classified. All seams of both wrappings must be sealed with brown sealing paper tape to aid in preventing undetected, unauthorized access to the contents while in transit.

2. Bulky Items – 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. Both the inner and outer containers will be marked as stated in the above paragraph.

3. Locked Briefcases – A locked briefcase is authorized for hand carrying of classified matter within the Washington, D.C. metropolitan area. If a locked briefcase is used to hand carry classified matter of any level, the briefcase may serve as the outer container (wrapper). The inner container shall be sealed, addressed with the sender's and recipient's classified mailing addresses, and marked with the overall classification level (and category if RD, FRD or TFNI) of the contents and with any appropriate caveats (see above paragraphs concerning packaging). The briefcase (outer container) must indicate the classified mailing address of the carrier and shall contain no markings to indicate that the contents are classified. A commercial luggage tag containing this address, affixed to the briefcase, is suggested.

   NOTE: A briefcase may not serve as the outer container for travel aboard commercial aircraft or when hand carrying or couriering classified matter to Congress or to an OGA when the intention is to leave the classified matter at the destination.

4. Tamper-Indicating Envelopes – Plastic tamper-evident security closures (bags, envelopes) are authorized for transmission of classified matter. For this use, tamper-resistant closures must meet all of the following criteria:

   - High strength coex film, or high strength Mylar type material, or equivalent
   - In-line closure
   - Opaque
   - Must not contain "zip open" feature.

Points to be considered when using tamper-indicating envelopes include:

- Standard classification and addressing markings must be applied
- The use of rubber stamps (for classification, addresses, etc.) is not permitted because the rubber stamp ink will not completely dry and will rub off or smear on the envelope's surface.
- Permanent markers (e.g., Sharpie permanent marker, or equivalent) should be used for classification markings and addresses.
- These envelopes may be used as the inner and/or outer wrapper(s) when hand carrying.
- These envelopes may be used as the inner envelope/wrapper when transmitting classified matter through the USPS, but not as the outer envelope or wrapper.
- These envelopes may be used for the inner and/or outer envelope(s)/wrapper(s) when transmitting classified matter via express mail. The package would then be placed within the appropriately addressed packaging (envelope or box) provided by the express mail carrier.
- External sealing tape is not required.
- Use of mailing labels is not recommended because some brands of stick-on labels do not adhere well to the coex film or Mylar and may detach in cooler temperatures.

5. Rifkin Safety Sac – The Rifkin Safety Sac® Document Handling Bag reusable key-locking fabric bag may also be used for hand carrying of classified material outside a facility.

Classified Mailing Addresses:

CMAs must be used for classified matter transmitted outside a HQ facility. These addresses are located in the SSIMS database and are valid for 30 days following the last database access.

NOTE: A mailing address for the inner envelope of a given facility may differ from the mailing address for the outer envelope for the same facility and addresses for USPS registered and certified mail may differ from that of express or common carrier mail for the same facility.

Transmittal of Classified Matter between HQ Facilities (Other Than Hand Carrying):

The Forrestal, 955 L'Enfant Plaza, and Germantown facilities are considered to be separate facilities; therefore, *non-hand carried* classified matter transmitted between these facilities must be handled by the element's CDCS. The CDCS uses their internal established procedures to coordinate with the mail room and/or HQ Courier Service to effect the transmittal.

Classified Document Receipts:

An appropriately prepared DOE F 470.10 Department of Energy, *Classified Matter Receipt*, must accompany all accountable and Secret documents transmitted outside a facility and must be enclosed within the inner envelope or container. If all items are going to one recipient, one receipt may be used for multiple items. Regardless of the number of items being transmitted, one receipt should be completed for each recipient. SSIMS must be consulted for appropriate and any special mailing instructions. All receipts should be Unclassified and should be prepared in triplicate, or quadruplicate if package is to be hand carried.

A record must be maintained for *all* classified matter, regardless of classification level, that is hand carried or couriered outside of an HQ facility. A DOE F 470.10 or equivalent manifest may be used to record the classified matter being hand carried or delivered to Congress.

Hand Carrying of Classified Matter within an HQ Facility:

Classified matter that will be hand carried to personnel located in a separate LA or VTR within the Forrestal, 955 L'Enfant Plaza, or Germantown facilities may be carried by personnel having an appropriate access authorization for the level and category of classified matter involved. The matter must have the appropriate cover sheet attached to the front of a document and appropriate markings (or an appropriate cover sheet) on the outside back page or cover. The matter must be transported within an HQ F 1410.5, *Classified Matter between Offices in DOE Headquarters*, red and white striped envelope. The HQ F 1410.5 must be marked with the recipient's name, room number, routing symbol, and telephone number.

The classified matter must be properly handled and protected while being hand carried. It should be under the constant and continuous protection of the authorized hand carry personnel until direct point-to-point delivery is made to the appropriate recipient or stored in the approved storage repository. There should not be any unnecessary convenience stops between destinations.

Hand Carrying of Classified Matter within a Limited or Exclusion Area:

Classified matter that will be hand carried to personnel located within the same LA or VTR within the Forrestal, 955 L'Enfant Plaza, or Germantown facilities may be carried by personnel having an appropriate access authorization for the level and category of classified matter involved. Transmittal is authorized with an appropriate cover sheet attached to the front of a

document and appropriate markings (or an appropriate cover sheet) on the outside back page or cover.

Hand Carrying of Classified Matter Outside a Facility within the U.S.:

The Head of each HQ Element must designate in writing a responsible official (e.g., the HSO) within the element to approve employees to hand carry classified matter out of a facility. This authority should be limited to as few people as operationally feasible.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter must maintain a record of those granted the authority to hand carry.

Only classified matter that is absolutely essential for the purpose (e.g., visit or meeting) may be hand carried. Alternatives to hand carrying must be considered. Options include USPS Registered Mail, express mail services, use of DOE authorized courier service, and secure facsimile.

Individuals hand carrying classified matter shall have an access authorization equal to or higher than the classification level and category of the classified information involved and be aware of their responsibility to protect classified information.

Travelers must not take classified matter to private residences or other unapproved places (e.g., hotel or motel rooms). Therefore, travelers who expect to arrive at the destination outside normal duty hours must be instructed to make prior arrangements for storage of classified matter through the host security office. All classified matter, when not in the possession of authorized individuals, must be stored only in DOE-approved facilities, or as specified in approved contingency plans. Arrangements shall be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter are required to ensure that each individual they authorize to hand carry is briefed on hand carrying responsibilities. A *Sample Briefing for Persons Authorized to Hand Carry Classified Documents* is provided in Sample 511-1. A record of hand carry briefings must be maintained. Each briefing must include, at a minimum:

- Packaging and addressing
- Transportation
- Protection of classified matter
- Transfer and receipting of classified matter
- Storage requirements, if applicable, for securing classified matter outside the HQ facility
- Procedures to validate through SSIMS that the hand carry destination is approved for the appropriate classified matter to be used, stored, discussed, etc., at the intended destination
- Handling and associated prohibitions (e.g., hotels, restaurants, residences, etc.)
- Reporting loss/compromise
- Contingency plans (inability to get to destination, traffic or other emergencies, route

diversions, alternate storage locations, etc.)
- Point(s) of contact for assistance.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter must provide approval each time classified matter is to be hand carried outside the Washington, D.C. metropolitan area. Repeated approval for hand carrying classified matter **within** the Washington, D.C. metropolitan area is not required and is valid until rescinded by the appropriate authority. Hand carrying classified matter **outside** the Washington, D.C. area is authorized provided that:

- The employee has received a hand carry briefing.
- An unusual situation warrants such action.
- The classified matter is not available or cannot be made available at the destination.
- Time does not permit transmission by other authorized means.
- The classified matter can be properly handled and protected while being hand carried.
- The transmission can be successfully completed on the same day.
- The classified matter can be appropriately stored upon arrival.
- Contingency plans for delayed arrival and unforeseen circumstances (e.g., unscheduled overnight delay outside the destination area, or weather delays) have been developed and approved by the Element. A *Sample Hand Carry Contingency Plan* is provided in Attachment 511-2.

A record is required for *all* classified matter, regardless of classification level, that is hand carried outside a facility. An **Unclassified** copy of this record must be in the possession of the employee who hand carries the classified matter, and a copy of the record must be maintained by the element's HSO or CDCS. The record may be a DOE F 470.10 or a locally produced manifest/record that identifies the classified matter being hand carried. The DOE F 470.10, manifest, or record must include:

- Subject or title
- Classification level and category of the matter being hand carried
- Date of the matter being hand carried
- Date the matter was removed from the facility
- Signature of the person removing the matter
- Date the matter was returned, transferred, or destroyed.

When the hand carrying employee returns to the facility, CDCS personnel must make a full reconciliation of the hand carried classified matter by reviewing the returned classified matter, receipts, and/or destruction certificates.

Hand Carrying Aboard Commercial Aircraft within the U.S.:

Classified matter may be hand carried aboard commercial passenger aircraft within the U.S. with the approval of the Head of Element or his/her designee. The purpose of the airport procedures outlined herein is to preclude the opening of classified packages by the Transportation Security

Administration (TSA) screening personnel. The Federal Aviation Administration (FAA) Advisory Circular dated 11/06/81 has been cancelled, and the TSA has replaced it with the guidelines below.

TSA Letter of Instruction to Carry Classified Material through a Screening Checkpoint at an Airport

The purpose of this guidance is to provide instruction to United States Government and contractor couriers on the procedures required to transport classified materials through TSA airport screening checkpoints.

Upon arrival at the screening checkpoint, ask a Transportation Security Officer (TSO) at the Travel Document Check or an available TSO stationed in front of the screening checkpoint to speak to the Supervisory Transportation Security Officer (STSO). The STSO will verify the courier's documentation, see list of required documentation below, and grant specialized screening of any classified materials carried by the courier. In order to transport U.S. Government classified material through a TSA screening checkpoint at an airport, a courier must present to the STSO all of the following items:

1) *Identification (ID) issued by his or her agency*
2) *A second piece of Government-issued photo ID*
3) *An authorization letter to carry the classified material from his or her agency with all of the following information:*

    (1) Full name of the agency
    (2) Full name of the courier
    (3) Date of issue and expiration date of the assignment
    (4) Full name, signature, and telephone number of the official issuing the letter, card, or form
    (5) Full name, signature, and telephone number of the official designated to confirm the letter, card, or form

In the event that an authorization letter, card, or form is not presented, or if the letter is missing any information listed above, or if the courier is not able to produce two forms of ID, as explained above, the material will not be permitted into the sterile area unless it has been properly screened.

Please note that only the U.S. Government classified material is eligible for specialized screening, the courier and any non-classified property carried by the courier is subject to screening. The STSO will ensure that any classified material is always within the line of sight of the courier during the screening process and is not subject to any additional inspection.

The authorization letter to carry the classified material must be from the Head of Element or his/her designee and must be on letterhead stationery. In addition to the original letter, the traveler should also have sufficient authenticated copies to provide a copy to each airline involved. A *Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material* is provided in Sample 511-3.

The classified package must be hand carried and not placed in checked baggage. The traveler is subject to normal screening procedures. Hand-held packages will normally be screened by x-ray examination. If security personnel are not satisfied with the results of the inspection, and the person hand carrying the material is requested to open a classified package for visual examination, the individual should inform the screener that the carry-on items contain U.S. Government classified information and cannot be opened. Under no circumstances may the classified matter be opened by the traveler or security personnel.

Hand Carrying of Classified Matter outside the U.S.:

Hand carrying of classified matter outside the U.S. is generally prohibited. However, in rare circumstances, the HQ CMPC Program Manager or the HQ DOE Cognizant Security Authority may approve the transmission on a case-by-case basis.

NOTE: Approval from the U.S. Department of State Bureau of Diplomatic Security (DS), Office of Diplomatic Courier Services (DS/C/DC) must also be obtained before classified matter may be hand carried outside the U.S.

Under no circumstances may classified matter be transmitted physically across international boundaries except by U.S. Department of State (DOS) diplomatic professional couriers or specifically DOS authorized nonprofessional couriers. Nonprofessional diplomatic couriers (e.g., DOE courier) may be authorized by DOS for international transporting **only in emergencies, when the professional DOS courier service will not cover the area into which the diplomatic pouch must be carried or the post to which the pouch is addressed within the time that official business must be conducted.**

Nonprofessional couriers must be U.S. citizens and full-time direct hire U.S. Government employees; have a Top Secret (or DOE "Q") security clearance, a diplomatic passport, a diplomatic visa, and diplomatic credentials bearing the seal and signature of the current Secretary of State; and have an E-country clearance with the notation that the courier is authorized to perform nonprofessional courier functions. Additionally, the classified material must be enclosed in sealed diplomatic pouches obtained from DS/C/DC until delivered to its official destination.

Several other conditions must be met before DOS will authorize a nonprofessional courier to hand carry classified matter across international borders. Contact the HQ CMPC Program Manager for additional information.

Transmittal of Classified Matter to Congress:

Classified documents must be hand carried to the U.S. Congress, since Congress has no CMAs.

The Office of Congressional and Intergovernmental Affairs (CI), the NNSA Office of External Affairs (NA-EA-10), and the Office of the Chief Financial Officer, Office of the Budget (CF-30), are solely responsible for the transmittal of classified matter to Congress. Consequently,

any deviation from the requirements listed below must be approved by the CI Director (CI-1), NA-EA-10, or CF-30. If a deviation from this policy is approved by CI-1, NA-EA-10, or CF-30 and if staff members from some other organization are authorized to hand carry classified matter to Congress, then the HQ CMPC Program Manager must train the authorized individual(s) in their courier responsibilities before they can courier the material.

With one exception, only appropriately cleared and designated employees of CI, NA-EA-10, and CF-30 are authorized to deliver classified matter to the Congress. When determining which HQ organization to contact to make arrangements for delivery of classified to Congress:

- CI-1 is the designated courier for DOE classified matter to Congress.
- CF-30 is the designated courier for ad hoc staff requests for classified matter addressed to the Senate Appropriations Committee or the House Appropriations Committee.
- NA-EA-10 is the designated courier for NNSA classified matter to Congress.

The one exception to the listing above applies to specifically designated and cleared NNSA personnel who are authorized to courier only the *Annual Report to Congress on DOE/NNSA Special Access Programs*. National policy requires that this annual report must be delivered to Congress by the Government Program Manager and/or the Government Program Security Manager, or their authorized representative, in coordination with the Special Access Program Oversight Committee (SAPOC) Executive Secretary, as appropriate. The SAPOC Executive Secretary should notify CI of the impending delivery.

The HQ Courier Service is not to be used for couriering classified matter to Congress. However, the HQ Courier Service may be used to transmit the classified matter from an HQ organization to the CI, NNSA, or CF points of contact. As soon as an organization becomes aware that it has an upcoming requirement for classified to be couriered to Congress, it should make telephonic contact with one of the CI, NA-EA-10, or CF-30 points of contact (see Points of Contact for Deliveries to Congress, below) to arrange for the delivery.

Packages for Congress must be properly wrapped and addressed through the appropriate DOE, NNSA, or CF point of contact to the name of the receiving member of Congress, Congressional Committee, or staff member. DOE F 470.10 (or equivalent) must be executed for *all* classified documents that are transmitted to Congress. Two copies of the receipt must be packaged within the transmitted envelope. A duplicate unclassified copy of the receipt should be made available for the courier to retain, and a fourth copy should be kept with the CDCS records.

NOTE: Documents intended for different members of Congress, different Congressional Committees, and/or different staff members must be individually packaged and wrapped and must contain separate receipts within each package. A separate DOE F 1410.6, DOE Messenger Receipt*, must be used for each separate package.*

Points of Contact for Deliveries to Congress:

- DOE:

  Patricia Temple, Legislative Affairs Specialist, Office of Congressional and Intergovernmental Affairs, CI-30, (202) 586-4220

  John Krohn, Director, Management and Operations, Office of Congressional and Intergovernmental Affairs, CI-1, (202) 586-7246

- NNSA:

  Joel Spangenberg, Acting Director, Office of External Affairs, (202) 586-8343

  Jason Miller, NNSA Deputy Director of Congressional Affairs, (202) 586-8368

- CF:

  Katherine M. Donley, Deputy Director for External Coordination, (202) 586-0176

Transmittal of Classified Matter to Foreign Governments and the International Atomic Energy Agency (IAEA):

The disclosure, release, and transfer of classified information to a foreign government is complex and requires the coordination and approval of several HQ organizations. Contact the HQ CMPC Program Manager for guidance.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (301) 903-9986 or (202) 586-4487

Forms/Samples/Graphics

Sample Briefing for Persons Authorized to Hand Carry Classified Documents (see Sample 511-1)

Sample Hand Carry Contingency Plan (see Sample 511-2)

Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material (see Sample 511-3)

HQ Form 1410.5, *Classified Matter between Offices in DOE Headquarters* ("Candy Striped Envelope"), available from the Forrestal and Germantown central supply stores (see Sample 511-4)

HQ Form 1410.6, *DOE Messenger Receipt* (available from the Forrestal and Germantown Transportation Offices)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to DOE Form 470.10, Classified Matter Receipt)

Other Reference

DOE Order 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*

Helpful Websites

To view the *DOE CMPC Marking Resource*, go to:
DOE CMPC Marking Resource

SAMPLE 511-1

Sample Briefing for Persons Authorized to Hand Carry Classified Documents

HAND CARRY OF CLASSIFIED MATTER BRIEFING
FOR OFFICE OF_____PERSONNEL

The following discussion is intended to assist you in discharging your security responsibilities when hand carrying classified matter.

Hand carrying of classified matter places significant security responsibilities upon you. You can avoid this situation by considering alternative means for transmitting the classified matter. These alternatives include sending the matter via courier, express mail, certified mail, or secure facsimile. Your servicing Classified Document Control Station (CDCS) Operators can assist you in transmitting the matter by these means. Hand carrying classified matter is authorized only when operationally necessary, not for convenience.

Hand carrying classified matter usually involves one of two types of situations:

- The person hand carrying the classified matter is merely a courier delivering the documents to a new custodian, where a transfer of custody is contemplated.
- The classified matter is to remain chargeable to the hand carrier during the period of removal from the office, and thereafter is to be returned to the hand carrier's office files.

The removal of classified matter from your office must be coordinated through your Headquarters Security Officer and/or servicing CDCS. Appropriate documents need to be generated on the classified matter you are hand carrying. It will take some time to generate these documents and instruct you in how to use them, so do not expect to have these requirements completed within a few minutes. You must also return to your CDCS when you have completed hand carrying the classified matter in order to reconcile your delivery records.

If you are hand carrying classified outside of the Washington, D.C. metropolitan area to/from either a DOE field site, an OGA, or the U.S. Congress, security clearances, SCI accesses, or Sigma accesses should be passed to the facility prior to arrival. This action, in conjunction with your standard DOE badge, may be used to verify authorization to hand carry classified matter.

If you are hand carrying only between the Forrestal and Germantown Buildings, your standard DOE security badge will be accepted as proof that you are authorized to hand carry classified matter. You should inform your HSO of your intention to hand carry between the two buildings and you ***must*** process through your CDCS to prepare the documents, package, and required labels. As stated above, you must also return to your CDCS when you have completed hand carrying the classified matter in order to reconcile your delivery records.

If classified matter is to be hand carried outside the Washington, D.C., metropolitan area, specific authorization from your HSO is required. You will need to furnish information about your travel plans and airline flights in order to generate the documents you will need to protect

the classified matter and still meet airport screening requirements. Again, these documents will take time to produce.

You will be given a Contingency Plan describing your responsibilities if there are travel difficulties, weather conditions, or other unforeseen circumstances that will significantly delay delivery of the classified matter. Review the Contingency Plan and keep it handy so you can find and comply with it when you really need it.

Your overall **responsibility** is to take all steps possible to ensure that the classified matter is not lost or otherwise compromised. You need to know that:

- Persons hand carrying classified matter must possess an access authorization commensurate with the level of information being hand carried and must be aware of their responsibility to continuously safeguard classified information.
- You must retain the classified matter in your personal possession AT ALL TIMES or store it – appropriately wrapped and sealed and subject to removal only by you or an appropriately cleared individual – in a DOE-approved repository.
- Taking classified documents to private residences is prohibited.
- Storing classified matter in hotel/motel rooms or safes, vehicles or their compartments, public lockers, or any other unapproved repository is prohibited.
- You may not make unnecessary convenience stops while transporting classified matter.
- All classified matter to be hand carried must be appropriately marked and wrapped.

If you lose or misplace any classified matter, or if it is compromised or possibly compromised, you must report the situation immediately to your HSO. If the incident occurs during non-working hours, you must notify, as soon as practical, the DOE Emergency Operations Center. If the incident occurs while you are attending classified meetings at other DOE or government facilities, you should also inform that facility's security officer or the security officer responsible for the meeting.

I acknowledge that I have read this briefing and understand my responsibilities for hand carrying classified matter:

_____	_____	_____
Printed Name	Signature	Date

SAMPLE 511-2

Sample Hand Carry Contingency Plan

Anyone hand carrying classified matter must be made aware of their organization's contingency plan for handling unexpected delays in the delivery of that matter. This is the contingency plan for personnel assigned to the Office of _____. This plan is not intended to cover all the circumstances that might occur; instead, it is a guide to help the individual cope with common delays such as traffic conditions, weather emergencies, and unexpected facility closings.

This contingency plan must be explained to, and a copy provided to Office of _____ personnel each time they hand carry classified matter.

Contingency Plan for Hand Carrying in the Washington, D.C. Metropolitan Area:

1. The DOE standard badge is the only document required to verify that the person is authorized to hand carry classified matter between DOE facilities in the Washington, D.C. area.

2. All classified matter must be double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the individual's Classified Document Control Station.

3. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* must be included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office's Classified Document Control Station. Station Operators will provide the required number of receipts or the manifest and provide instructions in how to use and return them.

4. If there will be an unusual delay in delivering classified matter, the person hand carrying the matter must contact his/her HSO and inform him/her of the situation. The Office of _____ HSO may be reached at _____during regular hours. After regular hours, or if the HSO is unavailable, the Emergency Operations Center can be contacted 24 hours per day at _____.

5. If the classified matter cannot be delivered promptly to the intended recipient, it must remain in the personal possession of the person hand carrying it. It *may not* be stored in the trunk of a car, a home, a hotel/motel room, a hotel/motel safe, a locker, or anything outside the personal control/possession of the person hand carrying it. *By deciding to hand carry the classified matter, the individual accepts full responsibility for ensuring the security of that matter. Responsibility cannot be transferred to any other person or organization without the approval of the HSO.*

6. If the classified matter cannot be delivered until after normal business hours, it may be taken to a DOE Protective Force Central Alarm Station (CAS) for safe storage. The CASs at the Forrestal and Germantown Buildings are the 24-hour classified matter receiving points for DOE facilities in the Washington, D.C. metropolitan area. The Forrestal CAS is in Room 1G-024 and the Germantown CAS is in Room A-060. The CAS will provide a hand receipt for the matter received. Do not lose this receipt because the CAS will demand return of the receipt before releasing it back to the person who delivered it.

7. If the classified matter cannot be retained by the person hand carrying it and it cannot be secured in an approved manner, the person should discuss the situation with the HSO for alternate instructions.

8. If hand carried classified matter is lost, stolen, misplaced, or otherwise cannot be accounted for, the HSO or the DOE Emergency Operations Center must be notified *immediately*.

Contingency Plan for Hand Carrying Outside the Washington, D.C. Metropolitan Area:

1. The person hand carrying classified outside of the Washington, D.C. metropolitan area to/from either a DOE field site, an OGA, or the U.S. Congress, should have his/her security clearance, SCI access, or Sigma access passed to the facility prior to arrival. This action, in conjunction with their standard DOE badge, may be used to verify authorization to hand carry classified matter outside the Washington D.C. metropolitan area.

2. The person hand carrying the matter must ensure that the intended destination is approved to handle, and store classified matter at the level and category being delivered. This check can be performed by Office of _____Classified Document Control Station Operators.

3. All classified matter must be double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the Office of _____ Classified Document Control Station.

4. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* must be included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office of _____ Classified Document Control Station. Station Operators will provide the required number of receipts or the manifest and provide instructions in how to use and return them.

5. If there will be an unusual delay in delivering classified matter, such as adverse weather conditions, lengthy airport/airline delays, or other emergencies, the person hand carrying the matter must contact his/her HSO and inform him/her of the

situation. The HSO may be reached at _____during regular hours. After regular hours, or if the HSO is unavailable, the Emergency Operations Center can also be contacted 24 hours per day at _____.

6. If the classified matter cannot be delivered promptly to the intended recipient, it must remain in the personal possession of the person hand carrying it until it is placed into secure storage. Secure storage is not the trunk of a car, a hotel/motel room, a hotel/motel safe, a locker, or anything other than the personal control/possession of the person hand carrying it or a repository approved for storage of the matter being carried. *By deciding to hand carry the classified matter, the individual accepts full responsibility for ensuring the security of that matter. Responsibility cannot be transferred to any other person or organization without the approval of the HSO.*

7. If the situation is such that the individual cannot properly protect the classified matter, the HSO can assist. Please contact the HSO at the number listed above. The HSO can request a search of the Safeguards and Security Information Management System (SSIMS) to determine whether any of the following secure facilities may be available to the traveler:
    a. A local DOE site approved for storing classified matter at the level and category being hand carried.
    b. A local DOE contractor facility approved for storing classified matter at the level and category being hand carried.
    c. A local U.S. military installation with the capability to store classified matter at the level and category being hand carried.
    d. A local FBI office with the capability to store classified matter at the level and category being hand carried.
    e. If none of these options are available, the traveler may be instructed to take the classified matter to a United States Post Office during business hours and mail the matter either to him/herself at DOE, to his/her HSO, or to the recipient via Registered Mail, as appropriate, using the DOE classified mailing addresses listed below (or the recipient's classified mailing address):

        Germantown Office
        ATTN: (Organization) (Intended Recipient)
        U.S. Department of Energy
        P.O. Box A
        Germantown, MD 20875-0963

        Forrestal Office
        ATTN: (Organization) (Intended recipient)
        U.S. Department of Energy
        P.O. Box 23865
        Washington, D.C. 20026-3865

8. If the classified matter is turned over to one of the above entities, the package must be closely inspected for signs of tampering or unauthorized opening once it is back in the

custody of the person responsible for it. If such signs are evident, the situation must be reported immediately to the HSO.

9. If hand carried classified matter is lost, stolen, misplaced, or otherwise cannot be accounted for, the HSO or the Emergency Operations Center must be notified *immediately*.

10. In emergency circumstances (such as natural disaster, terrorist attack, city evacuation, or any circumstances where appropriate storage or delivery as described above is absolutely not possible), common sense must apply in protecting the classified matter. In any situation or circumstance, you must personally protect the classified matter until it is appropriately secured at the earliest possible opportunity. In such emergencies, keep your HSO informed, and in all cases, you will be required to provide a report of the incident to your HSO as soon as you return to DOE HQ.

SAMPLE 511-3

Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material (Letterhead Stationery)

Date:

ADDRESSEE: TRANSPORTATION SECURITY ADMINISTRATION

SUBJECT: Letter of Authorization to Hand Carry Classified Material

This is to certify that the individual indicated below, who is an employee of the Office of _____, United States Department of Energy, is hereby authorized to hand carry classified matter related to National Security aboard a commercial aircraft.

Courier: Full Name
Agency ID: US Department of Energy
Dates of Issue and Expiration of Assignment: (dates of start and expiration of assignment)

Official Issuing
Authorization Letter: Full Name
Signature
Telephone Number

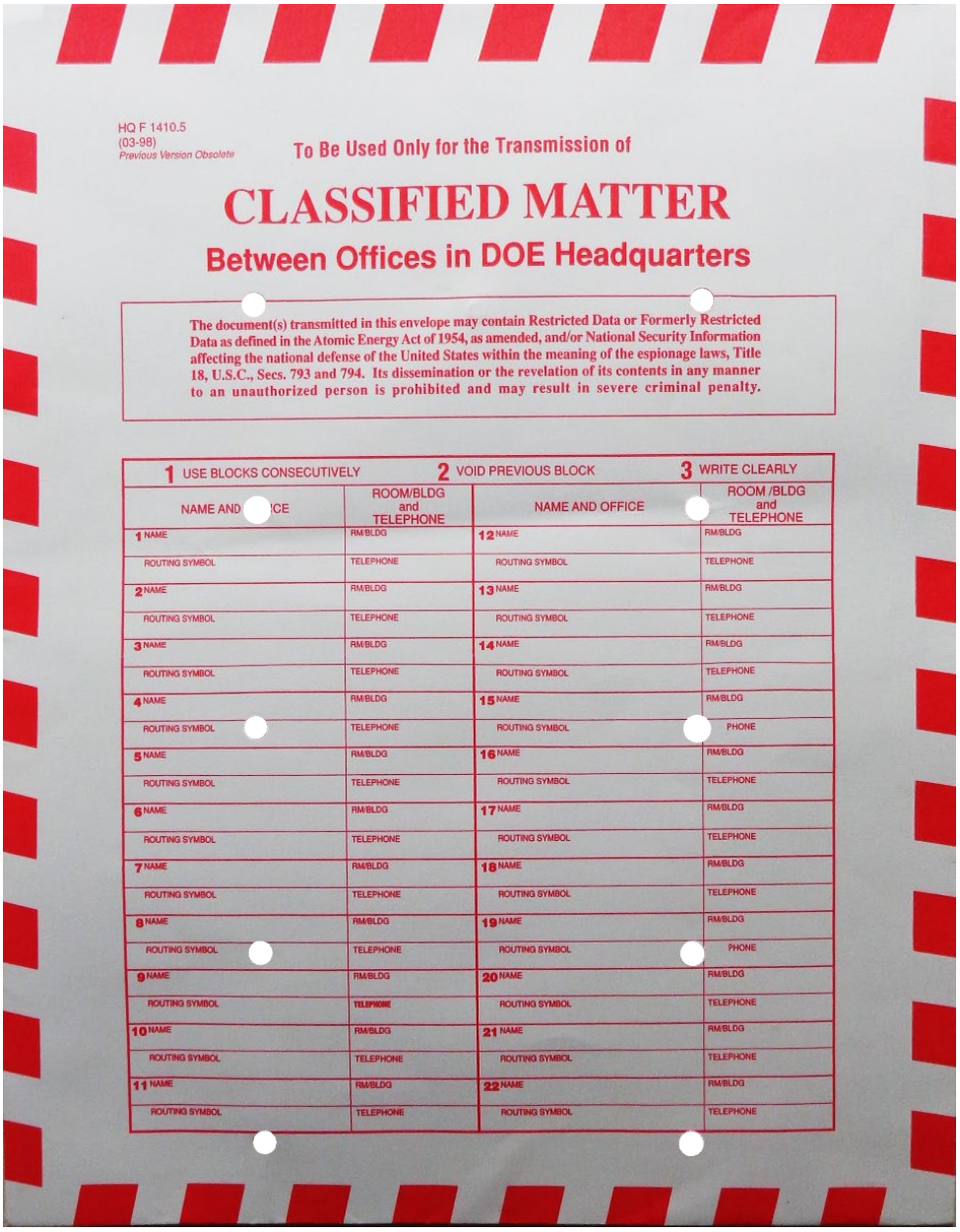
To Confirm
Authorization Contact: Full Name
Signature
Telephone Number

Sincerely,

Issuing Official Name
Issuing Officer Title

SAMPLE 511-4

Sample HQ Form 1410.5, Classified Matter between Offices in DOE Headquarters "Candy Striped Envelope"



HQ F 1410.5
(03-98)
Previous Version Obsolete

To Be Used Only for the Transmission of

CLASSIFIED MATTER

Between Offices in DOE Headquarters

The document(s) transmitted in this envelope may contain Restricted Data or Formerly Restricted Data as defined in the Atomic Energy Act of 1954, as amended, and/or National Security Information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Secs. 793 and 794. Its dissemination or the revelation of its contents in any manner to an unauthorized person is prohibited and may result in severe criminal penalty.

1 USE BLOCKS CONSECUTIVELY 2 VOID PREVIOUS BLOCK 3 WRITE CLEARLY

NAME AND OFFICE	ROOM/BLDG and TELEPHONE	NAME AND OFFICE	ROOM /BLDG and TELEPHONE
1 NAME	RM/BLDG	12 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
2 NAME	RM/BLDG	13 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
3 NAME	RM/BLDG	14 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
4 NAME	RM/BLDG	15 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	PHONE
5 NAME	RM/BLDG	16 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
6 NAME	RM/BLDG	17 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
7 NAME	RM/BLDG	18 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
8 NAME	RM/BLDG	19 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	PHONE
9 NAME	RM/BLDG	20 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
10 NAME	RM/BLDG	21 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE
11 NAME	RM/BLDG	22 NAME	RM/BLDG
ROUTING SYMBOL	TELEPHONE	ROUTING SYMBOL	TELEPHONE

This page intentionally blank.

Section 512
Classified Mailing Addresses

Classified matter must be addressed only to approved CMAs (i.e., mailing, shipping, or overnight express delivery) contingent upon the appropriate method of transmission. The CDCS operator must consult SSIMS to verify the CMA and the authorized storage capability of the receiver before dispatching the matter.

This section describes DOE HQ procedures for obtaining various CMAs.

HQ Implementation Procedures

It is recommended that each element have at least one CDCS operator designated to access SSIMS to acquire CMAs and to verify the approved classified storage capability of the receiving facility. This information is contained on DOE F 470.2, *Facility Data and Approval Record* (FDAR), which is stored in SSIMS. The form lists the receiving facility's Facility Clearance (Block 16); the authorized classified storage capability; classification level and category (Block 18); and the authorized CMAs for the method(s) of transmission that are authorized for the specific facility (Blocks 13, 17, and 20). CMAs verified through SSIMS are valid for 30 days from the date of validation. If no one in the HQ element has access to SSIMS, contact the Office of Information Security (AU-42). See the Points of Contact subsection below for information on contacting AU-42.

NOTE 1: SSIMS is an automated classified database that must be accessed through an information system approved and accredited to process classified information. Individuals requiring access to SSIMS should initially contact their ISSO, who will assist in locating an accredited system or provide assistance in accrediting a system to process classified data.

NOTE 2: To acquire SSIMS browser access and training, contact the SSIMS Administrator, Office of Security Assistance (AU-52). See the Points of Contact subsection below for information on contacting AU-52.

CMAs for HQ Elements:

CMAs for HQ elements are available in SSIMS. Each HQ element is registered in SSIMS as either a non-possessing or possessing facility. The FDAR for each HQ element reflects whether the element is authorized to receive classified matter at the Forrestal building, the Germantown building, or both locations. The FDAR also indicates the classification and category level of the HQ element's storage capability.

CMAs for Other DOE Federal Facilities:

CMAs for all non-HQ DOE facilities must also be verified in SSIMS. If the facility is able to receive classified matter, the FDAR reflects the classification and category level of storage capability and the CMA.

Contractor Facilities:

Companies that have contractual arrangements that require storage of classified matter in their contractor offices are registered in SSIMS as possessing facilities. The FDARs for possessing contractor facilities reflect the CMA and storage capabilities, as well as classified shipping and overnight addresses where appropriate.

Other Government Agencies:

CMAs for OGAs must be verified in SSIMS. The FDARs for OGA facilities reflect the CMA information, classified shipping, and overnight addresses (if appropriate), and the level of classification and category of matter the OGA is authorized to store.

OGA Contractors:

CMAs for OGA contractors must be verified in SSIMS. The FDARs for OGA contractor facilities reflect the CMA information, classified shipping, and overnight addresses (if appropriate), and the level of classification and category of matter the OGA is authorized to store.

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (202) 586-4487 or (301) 903-9990.

To contact the Office of Security Assistance (AU-52) to obtain access to SSIMS, call (301) 903-5108 or (301) 903-1163.

Forms/Samples/Graphics

DOE F 470.2, *Facility Data and Approval Record*

Section 513
Express Mail Service

Classified matter is sometimes transmitted through express mail; however, express mail packages cannot be marked as containing classified matter. Thus, there is a possibility that the recipient of an express mail package will not be aware that it contains classified matter and may not open it promptly or store it properly. To ensure that all express mail packages are opened promptly, that the contents are inspected, and that action is taken to properly store classified matter, it is DOE HQ policy for Express Mail Center personnel to release all express mail packages directly to the person to whom it is addressed (addressee) or to an Express Mail Document Control (EMDC) designee. If the addressee is not available, the express mail package must be released to another person who has been specifically appointed by the HQ element to receive and open such packages. Such individuals who are authorized to receive and open express mail on behalf of others within their organizations are known as EMDC designees.

NOTE: TS matter may not be transmitted via express mail.

NOTE: Commercial express mail service shall not be used as a matter of routine or convenience for transmitting classified matter. However, when such express service is deemed operationally necessary, CDCS personnel must follow their organization's procedures for transmitting a classified express mail package.

HQ Implementation Procedures

Appointment of Express Mail Document Control Designees:

Each HQ element must designate EMDC personnel before they can pick up express mail packages from the HQ Express Mail Offices on behalf of personnel within their organizations. The element's HSO must submit a list of the organization's EMDC designees to Office of Information Security. HSOs should use the *Sample E-Mail Notification for Express Mail Document Control Designees* (Attachment 513-1) to inform AU-42 of the element's EMDC designees. When there are changes in an element's list of EMDC designees, the HSO must immediately notify AU-42 of the changes by e-mail, using this same e-mail format.

NOTE: The Forrestal and Germantown Express Mail Offices are not authorized to release an express mail package to anyone other than the addressee, or an individual on the element's list of EMDC designees.

HQ elements are registered in SSIMS as either a possessor or non-possessor of classified matter:

1. Possessing Elements are HQ elements that can receive and store classified matter at the Forrestal, 955 L'Enfant, or Germantown facilities. EMDC designees from a Possessing Element must have a Q or L security clearance. CDCS personnel (see Section 510, Classified Document Control Stations) may also serve as EMDC designees.

2. Non-Possessing Elements are HQ elements that are not approved to receive or store classified matter at any of the HQ facilities. EMDC designees from a Non-Possessing Element are not required to possess either a Q or L security clearance.

Incoming Express Mail Packages to Possessing HQ Elements:

On the day the express mail package is received at HQ, the Express Mail Office at Forrestal or Germantown notifies the addressee via e-mail.

NOTE: This notification is an Express Mail Office practice that does not relate to security requirements.

Unless specifically prohibited by an organization (e.g., NA, AU, and SC), only the addressee or the cleared EMDC designees are authorized to retrieve packages from the Express Mail Office. Whoever retrieves the package is responsible for taking possession of the package, opening it, and inspecting it to determine whether it contains classified matter. If the package contains classified matter, it must be taken immediately to the element's CDCS for proper processing and/or storage. In any event, express packages must not be left unopened in an individual's inbox, on a desk, or in any other area awaiting attention by the intended recipient or some other person.

If the addressee or EMDC designee is unavailable or does not pick up the package by early afternoon of the following day, the Express Mail Office contacts the HSO for the recipient's organization and requests that arrangements be made for the package to be retrieved by a cleared EMDC designee or the addressee. On the morning of the third day, if the package has not been picked up by EMDC personnel or the addressee, the Express Mail Office notifies AU-42, which will decide what action to take on the undelivered package.

Outgoing Express Mail Packages from Possessing HQ Elements:

If an outgoing express package contains classified matter, it must be handled by the element's CDCS personnel. If the outgoing express package contains only unclassified matter, anyone can deliver the package to the servicing express mail office.

Incoming Express Mail to Non-Possessing HQ Elements:

On the day the express mail package is received at HQ, the servicing Express Mail Office at Forrestal or Germantown notifies the addressee. The addressee or EMDC designee is responsible for reporting to the Express Mail Office, taking possession of the package, and inspecting it to determine whether it contains classified matter. If it does, the HSO of the element must be notified, take possession of the classified matter, and seek guidance from AU-42.

If the package has not been picked up by early afternoon of the following day, the Express Mail Office contacts the designated HSO for the recipient's organization. On the morning of the third day, if the package has not been picked up, the Express Mail Office notifies AU-42, which will decide what action to take regarding the package.

Outgoing Express Mail from Non-Possessing HQ Elements:

Anyone can deliver an unclassified outgoing express package to the local Express Mail Office in accordance with the local element's procedures.

In the uncommon event that a non-possessing element must transmit classified matter via express mail, an appropriately cleared person (e.g., the HSO) must coordinate with the CDCS of a possessing element to effect this transmission.

EMDC Designee or Addressee Responsibilities:

EMDC designees or addressees must immediately pick up express mail packages when contacted by the Forrestal or Germantown Express Mail Office. Upon return to their respective office or designated security area, the EMDCs must immediately open the package and ensure that it does not contain classified matter.

To determine whether the package contains classified matter, first open the outer express package wrapping. If the material inside is not further wrapped and contains no classification markings, the material may be handled as unclassified. If classification markings are present, handle the package as classified matter as described below.

If the material inside contains an additional wrapping that is not marked with classification markings, open the inner wrapping. If there are no classification markings on the inner wrap, handle as unclassified. If classification markings are present, handle the package as classified matter as described below.

Packages with classification markings may only be opened by cleared personnel within designated approved security areas. If the addressee or EMDC designee does not meet these requirements, he/she must not open the package any further and must immediately contact the organization's HSO or CDCS personnel for additional guidance.

NOTE: If the individual cannot locate CDCS personnel, a cleared HSO, Alternate HSO, or HSO Representative, he or she must immediately contact AU-42 for assistance.

Point of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (202) 586-4487 or (301) 903-9990.

Forms/Samples/Graphics

Sample E-Mail Notification for Express Mail Document Control Designees (see Sample 513-1)

SAMPLE 513-1

Sample E-Mail Notification for Express Mail Document Control Designees

Send the e-mail to: Office of Information Security

The e-mail "Subject" block should be: "Notification of Express Mail Document Control Designees"

The body of e-mail should include the following information:

The Office of _____ has approved the following personnel to receive and open express mail packages addressed to this office:

Name of Designee:
Security Clearance Level:
Organization code and/or organizational name:
Building name:
Room number/location of Classified Document Control Station:
Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified mail and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO, Alternate HSO, or HSO Representative.

Information may appear in the following format (example):

FORRESTAL EXPRESS MAIL REGISTRY						
Element	Organization	Point of Contact	Phone #	Room No.	Action	Clearance
AU	Office of Environment, Health, Safety and Security					
	AU-1.23	John DOE	202-586-xxxx	1A-123	ADD	Q
		Jane DOE	202-586-xxxx	1A-123	DELETE	Q

This page intentionally left blank.

Section 514
Destruction of Classified Matter

This section describes how to properly destroy classified matter at DOE HQ.

HQ Implementation Procedures

HQ elements and support contractors should establish procedures for an ongoing review of their classified holdings to reduce their classified inventory to the minimum necessary. Multiple copies, obsolete matter, and other classified waste should be destroyed as soon as practical. Records disposition schedules, including the NARA General Records Schedule, and DOE records schedules must be taken into consideration before documents or other classified matter can be designated for destruction. If classified matter is under a court order prohibiting its destruction, guidance must be requested from the DOE Office of General Counsel.

Approved Methods of Destruction:

Classified matter must be destroyed beyond recognition to preclude reconstruction. The approved methods of destruction at HQ are:

1. Shredders – Crosscut shredders are approved for the destruction of all classified **paper documents**. The shredder must reduce the paper to a particulate size not greater than **1mm x 5mm** during the destruction process. The user should inspect the particulate output each time to ensure that the particulate size is no larger than 1mm x 5mm. Additionally, approximately every 6 months, HSOs are asked to check the particulate output of the shredders used by their elements to destroy classified matter. If the size requirement is not met, that particular shredder is taken out of operation until it can be repaired or replaced. Shredder residue meeting particulate requirements may be disposed of as normal unclassified (recyclable) waste.

   Crosscut shredders purchased prior to December 31, 2003, that produce residue with a particle size not exceeding 1/32" x 1/2" may continue to be used for the destruction of classified paper matter. If these shredders cannot be repaired or restored to cut residue within 1/32" x 1/2", they must be taken out of service.

   Crosscut shredders that produce a particulate size that meets the above requirement may be approved by the elemental HSO. Shredders approved by HSOs for classified destruction must be located in LAs or VTRs and must be designated by conspicuously posted signs. Shredders **approved** for classified destruction must have the sign posted either on the equipment or nearby. The sign must contain the make and model of the shredder and be signed and dated by the appropriate HSO. A sample of the sign is provided in Attachment 514-1. All shredders located in an LA or VTR that are **not approved** for destruction of classified matter must have a *Not*

Authorized for Classified Destruction sign posted on the shredder (a copy of this sign is provided on the Chapter 5 download page).

2. HQ Centralized Classified Destruction Facility (CCDF) – The CCDF is located at the Germantown, MD facility. It is used to destroy bulk amounts of classified or Controlled Unclassified Information paper documents and non-paper matter, such as audio and video tapes, viewgraphs, film, floppy disks, removable hard drives, and communication devices (e.g., Blackberry-type devices).

   NOTE 1: See Chapter 13, Controlled Unclassified Information (HQFMSP) for the destruction of CUI and unclassified Hard Drives.

   NOTE 2: Follow all organizational procedures before proceeding to destroy classified media.

3. Other Methods – On rare occasions, the CCDF may be unavailable for destruction operations (while undergoing maintenance or for other reasons). When the CCDF is not operating, the Director, AU-40, in consultation with the OCIO, may identify and approve alternative means of bulk classified destruction.

Destruction of Non-Accountable Classified Matter:

The destruction of non-accountable classified matter may be accomplished by one individual. No witness is required, and no record of destruction is required. The person doing the destruction must have a security clearance equal to or higher than the classification level, and category, and any other caveats, as applicable, of the waste material.

Preparation of Non-Accountable Classified Matter for Destruction:

Classified matter that cannot be destroyed on approved crosscut shredders located within HQ offices must be properly packaged and transported to the CCDF. The following guidelines should be followed for the destruction of **non-accountable classified matter**:

- Paper, plastics (including floppy disks), and metal (including metallic computer disks and removable hard drives) must be sorted into separate, properly annotated classified burn bags not to exceed 10 pounds in weight in Forrestal and 15 pounds in Germantown. Personally-owned, non-official waste materials, including food waste products, are not to be included in the burn bags. Failure to comply with destruction preparation procedures may result in the issuance of a security infraction.

  NOTE: Paper clips, heavy duty staples, and metal or plastic fasteners must be removed from all paper documents and waste. Bags containing fasteners of any kind will be returned to the originator.

- Classified burn bags are available in the DOE self-service supply rooms. They are recognizable by the red and white stripes on their outside surface. These bags are

designated **only** for classified waste. The name, routing symbol, telephone number, and room number of the person responsible for the burn bag, and the type of matter contained within (i.e., paper, plastic, or metal) must be clearly marked on the side of each bag for identification. The weight of the matter within each burn bag is limited to 10 pounds for those generated at the Forrestal Facility and 15 pounds for those generated at the Germantown Facility. The bags should be folded at least once and stapled shut every 2 inches. Burn bags are to be protected as classified matter until they are destroyed.

- Burn bags may be delivered to the following collection points during the times listed:
  - Forrestal Building – Room GI-007 between 3:00 p.m. and 4:00 p.m., Mondays, Wednesdays, and Fridays.
  - Germantown Building – Room R-002 between 9:30 a.m. and 10:30 a.m., Mondays, Wednesdays, and Fridays.

Destruction of Accountable Classified Matter:

The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter. Both the destruction official and the witness must have a security clearance equal to or higher than the classification level and category of the classified information to be destroyed. Facilities in which only one employee has the appropriate clearance must contact the HSO or AU-42 for guidance on destruction.

A DOE F 5635.9, *Record of Destruction*, or equivalent, must be completed whenever accountable classified matter is destroyed. An operator within the element's CDCS must authorize the destruction and maintain all DOE F 5635.9s or other destruction records/ receipts. Destruction certificates for accountable matter should be retained for 5 years for Top Secret and 2 years for Secret and Confidential.

Accountable matter may be destroyed with an HSO-approved crosscut shredder or at the CCDF. When using the CCDF, paper, plastics and metal must be sorted into properly annotated classified burn bags. The name, routing symbol, telephone number, and room number of the person responsible for the burn bag, and the type of matter contained within *(i.e., paper, plastic, or metal)*, must be clearly marked on the side of each bag for identification. Personally-owned, non-official effects, including food waste products, are not to be included in the waste matter. The bags should be folded at least once and stapled shut every 2 inches. Burn bags are to be protected as classified matter until they are destroyed.

A destruction appointment must be made by calling the CCDF operator at the phone number included in the Points of Contact subsection below. The CCDF operator will not sign the DOE F 5635.9 as the destruction official and cannot serve as the witness to the destruction. The HQ element destroying the accountable matter must provide both the destruction official and a witness to the destruction and both are responsible for transporting the waste to the CCDF for destruction.

See Section 509 for examples of accountable classified matter.

Points of Contact

For information about the HQ CMPC Program, contact the Office of Information Security or call (202) 586-4487 or (301) 903-9990.

To contact the Forrestal Collection Facility, call (202) 586-8600.

To contact the Germantown Collection Facility, call (301) 903-3910.

To make an appointment at the Germantown Centralized Classified Destruction Facility (CCDF), call 301-903-02035.

The following forms and graphics are available on the Chapter 5 download page:

Sample Authorized for Classified Destruction Sign

Sample Not Authorized for Classified Destruction Sign

Forms/Samples/Graphics

DOE Form 5635.9, *Record of Destruction* (for a copy of this form go to DOE Form 5635.9, Record of Destruction)