NOT MEASUREMENT SENSITIVE

DOE-HDBK-1223-2016

DOE HANDBOOK

Classified Matter Protection and Control Handbook

U.S. Department of Energy
Washington, D.C. 20585

AREA SANS

FOREWORD

The protection of classified matter is of paramount importance in fulfilling security responsibilities in connection with the Department of Energy (DOE). Classified matter includes documents, electronic media, and materials. Depending on the specific job responsibilities, employees may handle, use, or even generate classified matter. To ensure its protection, each employee should know and follow the applicable security procedures that implement the statutes, regulation, Executive Orders, government-wide policy directives and guidelines, and DOE policy and directives that are designed to protect and control classified information.

This handbook is not intended to replace DOE Order 471.6, *Information Security*, other departmental rules, plans or processes or national directives. This handbook describes one way to fulfill requirements for Classified Matter Protection and Control (CMPC) within DOE. Therefore, instead of the use of words such as "must" or "shall," the language would be that the resultant action "is" or "are." For example, instead of stating that "a classified cover sheet must be put on a classified document when it is removed from storage," it will state, "a classified cover sheet is put on a classified document when it is removed from storage" which is the result of following the requirement to use the classified cover sheet. It is important to understand this concept if using this handbook.

Section 1 describes the basic CMPC Program to include the roles and responsibilities of Federal employees and contractors who have access to, possess, or generate classified information. It also outlines the basic roles and responsibilities of those involved in administering the CMPC Program. It includes the various training requirements for personnel with security clearances or access authorizations and those performing specialized CMPC functions. Additionally, it provides information on exemptions and equivalencies as they apply to the CMPC program.

Section 2 briefly describes the classification program and the requirements for classification reviews.

Section 3 describes the three levels of classified information and four categories of classified information in use throughout the U.S. government, special designators unique to DOE, and other special handling controls.

Section 4 describes the specialized topic of identifying and handling classified or sensitive information generated by foreign governments.

Section 5 describes the procedures for preparing and marking classified matter.

Section 6 describes how to protect classified matter while it is out of its normal storage container and in use.

Section 7 describes the procedures and equipment used to properly store classified matter.

Section 8 describes the procedures for reproducing classified matter and identifying the equipment.

Section 9 defines what classified matter is accounted for and the accountability mechanisms used.

Section 10 establishes a Classified Matter Control Station(s) (CMCS) as necessary to centrally manage the receipt or transmission of classified matter. Including general operating instructions and training requirements for CMCS operators.

Section 11 describes the procedures for receiving and transmitting classified matter, including the mailing, hand carrying, and electronic transmission of classified matter.

Section 12 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 13 deals with the use of Express Mail Services to send and receive classified matter.

Section 14 describes the procedures and equipment to destroy classified matter.

Section 15 describes Incidents of Security Concern (IOSC) and immediate response activities.

At the end of each section, there may be suggested points of contact and helpful websites that may provide additional information. Any examples referenced in a section are also found at the end of that section.

TABLE OF CONTENTS

INTENTIONALLY LEFT BLANK

Section 1
Classified Matter Protection and Control Program

The Classified Matter Protection and Control Program (CMPC) is based on the single goal to deter and detect access to classified information by unauthorized individuals. This is done with the cooperation of the individuals who have been granted appropriate security clearances or access authorizations by the U.S. government and 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 the appropriate security clearance or access authorization and relevant access approval that permits access to the classified matter? and 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; training and security education of those employees, as well as exemptions and equivalences and other potential variations to national policy.

The Officially Designated Federal Security Authority (ODFSA) is responsible for reviewing security plans and ensuring the supporting analysis is complete and accurate before concurring or approving as appropriate. Exemptions and equivalencies may be considered when the requirement is derived from Department of Energy (DOE) Order (O) 471.6, Admin Chg 2, *Information Security*. Equivalencies and exemptions from that Order are processed in accordance with DOE O 251.1C, *Departmental Directives Program*. The process for deviating from national requirements is found in the source document.

If the source document does not provide a deviation process, the DOE Office of General Counsel or the National Nuclear Security Administration (NNSA) Office of General Counsel will be consulted to determine whether deviations from the national requirement can be legally pursued.

Roles and Responsibilities:

Officially Designated Federal Security Authority (ODFSA) and Officially Designated Security Authority (ODSA).

The ODFSA is a Federal employee with delegated authorities and responsibilities for assigned CMPC duties. The ODFSA is designated as the primary point of contact for specific CMPC activities within the Headquarters (HQ) Departmental Element/Program Office by a formal delegation of authority memorandum. The ODFSA is responsible for ensuring CMPC procedures to implement the requirements of applicable laws, Executive Orders, and DOE

directives are developed for each site or facility under their responsibility and within their delegated authority. The ODFSA may further delegate other personnel to fulfill assigned duties through a delegation of authority memorandum. While an ODSA may be a Federal or contractor employee, contractors may not be delegated inherently Federal governmental duties and responsibilities. If a task is further delegated, the delegator remains responsible for all tasks originally delegated to them, including those delegated to others.

Other CMPC-related Roles. Other Federal or contractor employees who have general responsibilities related to the protection and control of classified information at most sites or facilities discussed in this document include, but are not limited to:

- Personnel accessing, using or creating classified documents;
- Classified Matter Control Station (CMCS) operators;
- Custodians;
- Derivative Classifiers;
- Classified matter couriers; and
- Mailroom personnel

Performance Plan Element for Federal Employees with Security Clearances or Access Authorizations:

All Federal employees who hold a Top Secret (TS), Secret (S), or Confidential (C) security clearance or a "Q" or "L" access authorization have an element in their Performance Plans describing their responsibilities for protecting classified information. A commonly accepted Performance Plan Element includes:

- Goal Linkage: Ensure that classified information is protected under conditions that deter and detect compromise or access by unauthorized persons;
- Results-Focused Critical Element with Credible Measure(s): Properly handles, classifies, processes, stores, reproduces, transmits, and destroys classified information to prevent its loss, compromise, or unauthorized disclosure; and
- Weight: The weight or significance assigned to this element is determined by the employee's supervisor.

Training and Security Education:

Security Briefing

Executive Order 13526, Title 32 Code of Federal Regulations (CFR) 2001 and DOE directives (e.g. DOE O 470.4B Chg1 and DOE O 471.6 Admin Chg 2,) require that all individuals who are authorized to access classified information receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable of their responsibilities and applicable requirements. This is provided in a Comprehensive Security Briefing at DOE (see Note below). This briefing includes instruction and information regarding:

- Known threats against the Department;
- Counterintelligence awareness;
- Cybersecurity awareness;
- The security classification system;
- Employee reporting obligations and requirements, including Insider Threat;
- Proper handling and storage of classified matter;
- Access control procedures for security areas;
- Escort requirements;
- Penalties for mishandling classified information;
- Controlled articles; and
- Basic security procedures and duties applicable to the employee's job.

NOTE: Although 32 CFR 2001 states that "Initial" training as described above shall be provided to every person who has met the standards for access to classified information in accordance with section 4.1 of the Order, within DOE there are two separate required briefings: an Initial and a Comprehensive Security Briefing. The Initial Security Briefing is provided to both cleared and uncleared employees who require access to a DOE or DOE Contractor site/facility. In addition, those employees who require access to classified, also receive a Comprehensive Security Briefing, which includes the information listed above.

Upon completion of the Security Briefing outlined above, the employee reads and signs the SF-312, *Classified Information Nondisclosure Agreement*, with the briefing official signing as the witness. The signed SF-312 documents the employee's completion of this security briefing. Any employee who fails to complete the SF-312 may have his/her security clearance or access authorization administratively withdrawn and will be denied access to classified matter until such time as the form is completed (signed). The records of who completed the briefing and their signed SF-312s are retained for a period of 70 years.

Annual Security Refresher Briefing

All employees, both Federal and contractor, with a TS, S or C security clearance or "Q" or "L" access authorization complete an Annual Security Refresher Briefing. This briefing summarizes the information provided during their Comprehensive Security Briefing along with new threat information or protection requirements, which may need updating based on self-assessment and survey findings, program changes, etc. Personnel who are required to receive the briefing are reminded of the requirement and advised on how to access the briefing, provided a date for completion, and advised how to print a completion certificate or obtain other certification of training. There is an audit capability to track who has completed the briefing. Those who are required to complete this briefing are tracked to ensure 100% completion rates.

Specialized CMPC Training/Briefings

Title 32 CFR Part 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. The CFR further states: "The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, on-line presentations, and other media and methods. Each agency shall maintain records about the programs it has offered and employee participation in them."

Within DOE, the terms "training" and "briefings" are used to differentiate between the training described in DOE O 470.4B and the briefings often provided locally. In addition, specialized briefings are provided for Classified Matter Control Station(s) (CMCS) operators; classified matter couriers; and mailroom personnel. Specialized CMPC training and/or briefings 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.

It is the responsibility of the Head of HQ Departmental Element/Program Office, Field Office or their designee to determine which of their employees require specialized CMPC training and ensure that the identified employee(s) complete the training as required. Note that specialized training requirements may change (e.g., when an employee is assigned new security responsibilities or when an employee is involved a security incident regarding the mishandling of classified matter, etc.).

The ODFSA is responsible for ensuring that specialized CMPC training courses are located or developed and that the training is available to Federal and contractor employees as needed.

Examples of training courses or briefings may include, but are not limited to:

- CMCS operations;
- Classified matter courier operations;
- Procedures for hand carrying classified matter; and
- Escort responsibilities.

Upon request, the ODFSA may also develop and provide specialized CMPC courses for organizations with unique requirements.

Specialized training courses should be available throughout the year. Employees are advised when these training opportunities are available and may recommend other personnel to attend. Additionally, organizational management 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 and other related courses that support the CMPC program. The HQ Departmental Element/Program Office is responsible for sponsoring and funding the attendance, travel, and other actions associated with their personnel attending all required training (both locally developed and NTC courses). NTC delivers their training in Albuquerque and in a variety of other ways, including computer-based training, correspondence courses, and mobile training teams. 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.

Exemptions, Equivalences and other Variations to Policy:

General

Equivalencies are alternatives to "how" a requirement in a directive is fulfilled in cases where the "how" is specified. These represent an alternative approach to achieving the goal of the directive. Unless specified otherwise in the directive, equivalencies are granted, in consultation with the Office of Primary Interest (OPI), by the Program Secretarial Officer or their designee, or in the case of the NNSA, by the Administrator or designee, and documented for the OPI in a memorandum.

Exemptions are the release from one or more requirements in a directive. Unless specified otherwise in the directive, exemptions are granted, in consultation with the OPI, by the HQ Departmental Element/Program Secretarial Officer or their designee, or in the case of the NNSA, by the Administrator or designee, and documented for the OPI in a memorandum. For those directives listed in Attachment 1 of DOE O 410.1, *Central Technical Authority (CTA) Responsibilities Regarding Nuclear Safety Requirements*, CTA concurrences are required prior to the granting of Exemptions.

The basis for approving exemptions and equivalency requests are documented in the approval memorandum. Any increase in risk to public health and safety, the environment, workers, or security is justified.

Any time there is a request for an exemption from or equivalency to the procedures in the national or DOE policies, the ODFSA is responsible for reviewing and ensuring the supporting analysis is complete and accurate before concurring on and forwarding that request as appropriate.

Equivalencies and exemptions from the requirements of DOE Order 471.6, Admin Chg 2, *Information Security*:

Equivalencies and exemptions related to DOE Order 471.6, Admin Chg 2, are processed in accordance with DOE O 251.1C, *Departmental Directives Program*. Requests for equivalencies or exemptions from the requirements in DOE Order 471.6, *Information Security*, are supported by a vulnerability assessment (VA) when required by the assets being protected, and by sufficient analysis to form the basis for an informed risk management decision regarding any potential increase in risk to public health and safety and environment, workers, or security.. The analysis identifies compensatory measures, if applicable, and/or alternative controls to be implemented.

All approved equivalencies and exemptions under DOE O 471.6, Admin Chg 2, *Information Security*, are entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security plan(s). Approved equivalencies and exemptions are a valid basis for operation when they have been entered in SSIMS, documented in the appropriate security plan, and incorporated into site procedures at that time.

Equivalencies and exemptions from the requirements in National Directives

Many DOE Safeguards and Security (S&S) Program requirements are found in or based on regulations issued by Federal agencies and codified in the CFR, or other authorities, such as Executive Orders or Presidential Directives (national source documents). Requests for deviations from requirements found in national source documents are processed as described in the applicable document.

These requests are processed through the ODFSA and Program Office/ HQ Departmental Element in the same manner as equivalencies and exemptions to DOE directives, with the only difference being the approval authority as outlined in the specific national directive from which the change is being sought.

You may contact the Office of Security Policy to ensure that the appropriate pathway is followed for the alternative that is requested.

Points of Contact:

For the names and contact information for those who occupy the positions identified in this section, contact your ODFSA.

Helpful Websites:

For information on classes available at the NTC, go to: https://ntc.doe.gov/

For information on training classes available at the Information Security Oversight Office, go to: http://www.archives.gov/isoo/training/

For information on training offered by Center for Development of Security Excellence, go to: http://www.cdse.edu/index.html

For information on training offered by National Counterintelligence and Security Center, go to: http://www.ncsc.gov/training/wbt.html

For information on the national and Departmental policy drivers go to: https://pir.doe.gov/collections

INTENTIONALLY LEFT BLANK

Section 2
Classification

Department of Energy (DOE) Order (O) 475.2B, *Identifying Classified Information*, establishes DOE's program for classifying and declassifying information and specifies requirements and responsibilities for implementing this program. This handbook summarizes the basic procedures for classifying and declassifying information, documents, and material, as well as the associated processes, such as classification training, classifier appointments, and authority descriptions. The details of those procedures are found in the above referenced Order.

Implementation Guidance:

Federal and contractor elements that have employees who generate classified information, documents, or material have either a Program Classification Officer (PCO), Classification Representative (CR), or a Classification Officer (CO) to assist individuals at the organizational element with implementing the requirements in DOE O 475.2B, *Identifying Classified Information*. For assistance in identifying the applicable PCO, CR or CO for your organizational element or for help with nominating an official for appointment, contact the Office of Classification's (AU-60) Outreach Program at (301) 903-7567 or outreach@hq.doe.gov.

Any matter that potentially contains classified information and is not intended for public release is reviewed by a Derivative Classifier (DC) with the appropriate authority. Prior to that review, if the document is expected to be revised, it is dated when created, marked with the highest potential classification level and category (if Restricted Data (RD), Formerly Restricted Data (FRD), or Transclassified Foreign Nuclear Information (TFNI)), and marked as a draft or working paper on the front cover or page. (See Section 3 for category definitions.) Any matter in a classified subject area that is intended for public release is reviewed by a CO or a DC who has been delegated this authority.

When a document needs to be classified or declassified, if a DC or Derivative Declassifier (DD) with appropriate authority is not known, the person who needs the document reviewed will contact the local PCO, CR or CO, as appropriate; or the AU-60 Outreach Program to determine who the DCs or DDs are within the organizational element or location.

Before a classified document or an extract from a classified document can be declassified or have classified information removed to create an unclassified version (i.e., redacted version), it is reviewed by the appropriate authority in accordance with Attachment 4 of DOE O 475.2B, *Identifying Classified Information*.

When information within a document is determined to require classification at a higher level and/or category, the document is upgraded by an appropriate authority..

Downgrading occurs when the information in the document can be protected at a lower classification level or category than what is currently marked on the document. The upgrading determination is made by a DC while the downgrading determination is made by a DD. Once these determinations are made, the DC or DD, respectively, notifies the originator or the custodian of the document so that the markings can be changed on other copies. Individuals who receive upgrading or downgrading notices do not require DC or DD authority in order to change the markings on a document. It is, however, extremely important to ensure that the document identified on the notice has been located and is the appropriate document before any markings are changed. When documents are declassified, a declassification notice is also sent following the same process. When a document is upgraded (particularly when it was previously issued as unclassified), it is important to follow proper procedures for notifying the appropriate security official who will determine whether or not the information has been compromised. Communication about documents that were not properly protected can themselves be classified.

All documents in a classified subject area that are intended for public release (e.g., for a publicly available webpage, for news organizations, etc.), including documents provided to or testimony given to Congress are reviewed by the CO or by a DC who has been delegated authority in writing. Documents being provided to Congress may also require review by AU-60 or the National Nuclear Security Administration Office of the Associate Administrator for Defense Nuclear Security (NA-70).

Points of Contact:

For information about the Classification Program, call (301) 903-7567 or E-mail outreach@hq.doe.gov.

Helpful Websites:

The Office of Classification's website is at: http://energy.gov/ehss/services/classification

To view the *DOE CMPC Marking Resource*, go to:
http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

To view the ISOO Marking Classified Information Booklet, go to:
http://www.archives.gov/isoo/training/marking-booklet.pdf.

Section 3
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 Department of Energy (DOE).

Access to Classified Matter:

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

General:

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 three levels and four categories of classified matter. Classified information may be conveyed in various forms, such as spoken word, documents, media, parts, weapons systems or other matter.

Levels of Classified Information:

Top Secret (TS) – The Top Secret classification level is applied to information the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security.

Secret (S) – The Secret classification level is applied to information for which the unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Confidential (C) – The Confidential classification level is applied to information, for which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

Categories of Classified Information:

The following are the terms in use throughout the U.S. government, special designators unique to DOE, and other special handling controls:

Restricted Data (RD) – All data concerning design, manufacture, or utilization of atomic weapons; production of special nuclear material (SNM); or use of SNM in the production

of energy, excluding data declassified, and data removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended (AEA). (https://powerpedia.energy.gov/wiki/Atomic_Energy_Act_of_1954)

Formerly Restricted Data (FRD) – Classified information jointly determined by the Department of Energy or its predecessor agencies and the Department of Defense to be related primarily to the military utilization of atomic weapons, and can be protected in a manner similar to National Security Information.

Transclassified Foreign Nuclear Information (TFNI) – Classified information concerning the nuclear energy programs of other nationals (including subnational entities) removed from the RD category under section 142(e) of the AEA after the DOE and the Director of National Intelligence (DNI) jointly determine that it is necessary to carry out intelligence-related activities under the provisions of the National Security Act of 1947, as amended, and that it can be adequately safeguarded as National Security Information.

National Security Information (NSI) – Any information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information* (http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf), or any predecessor order, to require protection against unauthorized disclosure and that is so designated.

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.

Caveats

- Foreign Government Information (FGI) – See Section 4, 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 matters;

    - No Foreign Dissemination (NOFORN); it is also to be used in all cases on Naval Nuclear Propulsion Information (NNPI) documents (both classified and unclassified),
    - Originator Controlled Information (ORCON),
    - Proprietary Information (PROPIN),
    - Authorized for Release To (REL TO); used to denote acceptable foreign national access, and
    - 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.

Special Controls

- North Atlantic Treaty Organization (NATO) has four levels of classification;

  - COSMIC Top Secret,
  - NATO Secret,
  - NATO Confidential, and
  - NATO Restricted.

  NATO also distinguishes official, unclassified information using the classification NATO Unclassified.

  The classification ATOMAL is used in conjunction with COSMIC Top Secret, Secret, and Confidential.

- Cryptographic (CRYPTO) may be used in conjunction with DOE O 470.6, *Technical Security Program* and other programs;

- Weapon Data;

  - Sigma Category (SIGMA) (14; 15; 18; 20), and

  - Critical Nuclear Weapons Design Information (CNWDI) – Department of Defense designation for TS/RD or S/RD weapon data that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munitions, or test device,

- Naval Nuclear Propulsion Information – NNPI may be classified or unclassified and is annotated NOFORN;

- Special Category (SPECAT) – Special Categories include: Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, Restricted Data (RD), or other compartmented information when used in conjunction with DOE O 470.6, *Technical Security Program* and other programs;

- Special Access Programs (SAPs) – A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level;

- Dissemination and Reproduction Notices;

- FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY, or

- REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR.

Points of Contact:

For information about the types of classified matter, contact your ODFSA or call (301) 903-2661 or E-mail Security.Directives@hq.doe.gov.

For information on NATO access, contact the Office of Resource Management and Mission Support, Headquarters Security Operations, or call (301) 903-9397.

Helpful Websites:

To view DOE Order 471.6, Admin Chg 2, *Information Security*, go to: https://www.directives.doe.gov/directives-documents/400-series/0471.6-BOrder-admchg2

To view the *DOE CMPC Marking Resource*, go to: http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

To view the *ISOO Marking Classified Information Booklet*, go to: http://www.archives.gov/isoo/training/marking-booklet.pdf.

Section 4

Classified Foreign Government Information

This section describes procedures for identifying and handling Foreign Government Information (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, governments, 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 and is safeguarded in compliance with NATO procedures (United States Security Authority for NATO Affairs [USSAN] 1-07).

Implementation Guidance:

General

FGI as defined by Executive Order 13526, is classified national security information. Information on foreign nuclear programs may be Transclassified Foreign Nuclear Information (TFNI). The release or disclosure of classified National Security Information (NSI) FGI or TFNI to any third country has the prior consent of the originating government according to treaty, agreement, bilateral exchange, or other obligation.

FGI containing Restricted Data (RD) or Formerly Restricted Data (FRD) is not NSI and release to any third country is governed by the Atomic Energy Act.

FGI retains its original classification markings or is 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 Classified Matter Protection and Control Program (CMPC) Marking Resource Foreign Government Markings Table.)

The release or disclosure of any FGI has the prior consent of the originating government, is coordinated through the cognizant DOE Program Office/HQ Departmental Element and the

Office of Environment, Health, Safety and Security and complies with all applicable treaties, agreements, or other obligations.

Any individual receiving FGI possesses an appropriate security clearance or access authorization and meets need-to-know requirements.

If the release or disclosure involves FGI produced by or received from another government agency (OGA), approval is obtained from that OGA before release or disclosure.

Top Secret (TS)/FGI, Secret (S)/FGI, and Confidential (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 on 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 is reviewed by a Derivative Classifier (DC), and an equivalent U.S. classification is 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 if identified as or marked with equivalent foreign government markings as found on the list of "Equivalent Foreign Security Classifications" in the CMPC Marking Resource document. Documents generated by DOE personnel that contain FGI are 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, a newly created classified document containing FGI and U.S. information is portion marked.

Accountability of FGI

TS/FGI – All TS/FGI is accountable. Reproduction requires the consent of the originating government. Destruction is accomplished by two individuals and a Destruction Certificate is completed by both individuals to record the actual destruction. (See Section 9, Classified Matter Accountability, for more information on accountability requirements.)

S/FGI – S/FGI records are kept for receipt, external transfer, destruction, and reproduction. Unless prohibited by the originator, S/FGI may be reproduced, and reproduction is recorded unless that requirement is waived by the originator. Destruction is accomplished by two individuals, and a Destruction Certificate is completed by both individuals to record the actual destruction.

C/FGI – Accountability records are not 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 designated Confidential – Modified Handling Authorized (C/FGI-MOD), and so marked on the first page. A DOE F 470.9, *C/FGI-MOD Cover Sheet*, is used on C/FGI-MOD documents only. The country of origin is indicated at the bottom of the cover sheet. The marking on the first page of the document is as follows,

This document contains (*insert name of country*) (*insert foreign 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 are provided appropriate handling instructions, either via a briefing from the ODFSA or their designee responsible for the program involving the C/FGI-MOD, or via written instructions on an approved C/FGI-MOD cover sheet, DOE F 471.2 (http://energy.gov/NODE/336811).

Information systems that store and/or process C/FGI-MOD are never accessed or serviced by foreign nationals.

When not in use, C/FGI-MOD is 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. Those with access to C/FGI-MOD ensure there is no 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 is transmitted in the same manner as classified matter unless this requirement is waived by the originating foreign government.

C/FGI-MOD information is destroyed in the same manner as classified information (see Section 14, Destruction of Classified Matter).

Points of Contact:

For information about FGI, contact the ODFSA, or e-mail the Office of Security Policy at: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Copies of DOE forms can be found as follows:

To view all DOE forms, go to:
http://energy.gov/cio/office-chief-information-officer/services/forms

DOE Form 471.2, *C/FGI-MOD Cover Sheet* --
http://energy.gov/sites/prod/files/DOE%20F%20471.2.pdf) or
http://energy.gov/NODE/336811

Helpful Websites:

To view the *DOE CMPC Marking Resource*, go to:
http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

To view the *ISOO Marking Classified Information Booklet*, go to:
http://www.archives.gov/isoo/training/marking-booklet.pdf.

Section 5
Marking Classified Matter

This section describes Department of Energy (DOE) procedures for marking classified matter. Regardless of the date or agency of origin, classified matter is marked to indicate at least the classification level and category (if Restricted Data (RD), Formerly Restricted Data (FRD), or Transclassified Foreign National Information (TFNI). All classified documents dated **before** April 1, 1996, are marked in accordance with directives in place at the time of origin.

Documents containing RD and/or FRD generated **before** July 9, 1998, are re-marked to indicate the category on each page if the documents are sent outside the office of origin or holder for other than archiving purposes. Documents containing RD and/or FRD generated **after** July 9, 1998, have the category marked on each page.

Implementation Guidance:

General

The markings that are common to all classified documents include;

- Classification level,
- Classification category (if RD, FRD, or TFNI),
- Caveats and special control markings (when required),
- Originator identification,
- Title/Subject marking,
- Unique identification numbers (for accountable matter only),
- Portion marking (for documents containing NSI or TFNI that does not contain RD or FRD), and
- Classification Authority Block (provided by the DC see Note 2 below).

Consult the *DOE Classified Matter and Protection Control (CMPC) Marking Resource*, the Information Security Oversight Office (*ISOO) Marking Classified Information Booklet* and the *Guideline for Marking Email on a Classified Network* for examples of how to properly mark classified matter in its various forms. Information on these resources can be found at the end of this Section.

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 National Security Information (NSI) documents with the exception of documents generated by DOE that contain only NSI which must also have the special control marking "Derivative Declassifier review required prior to declassification" on the first page. This marking is required in order to prevent the

inadvertent release of RD, FRD, or TFNI and to ensure that the NSI classification has not been extended per section 3155 of Public Law 104-106, which states: "Before a document of the Department of Energy that contains national security information is released or declassified, such document is reviewed to determine whether it contains restricted data," and DOE O 475.2B, Identifying Classified Information. If a classified document is originated by DOE, it is 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 are marked with the overall classification level and the appropriate cover sheet identifying the classified information is used. Resolution of OGA deficiencies and/or continuing patterns of deficiencies should be handled through the ODFSA.

NOTE 2: All classified documents (other than Working Papers or draft documents – see below) 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 Derivative Classifier (DC) makes the classification determination for the original copy of each document. Any change to a classified document that may result in a higher level/classification is reviewed by a DC. The placement of a DC's name on a classified document without the DC's direction or authorization will result in an inquiry and/or investigation. Consult DOE Order 475.2B, Identifying Classified Information for additional information on identifying classified information.

NOTE 3: All NSI documents and all page changes to NSI documents created after April 1, 1997, are portion marked, unless based on compilation. (In compilation, a large number of similar unclassified or unclassified and classified pieces of information, the selection, arrangement or completeness of which adds sufficient value to merit classification or classification at a higher level and category.)

Classified Cover Sheets

At a minimum, all classified documents include the appropriate cover sheet (Top Secret, Secret, Confidential or C/FGI-MOD) attached depicting the classification level of the classified matter whenever that document is outside a General Services Administration (GSA)-approved security repository. Additionally, the back of all classified documents also include the 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 (SF) 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 7, Storage of Classified Matter, for instructions on how to mark SF-700s.

Marking Electronic Files and E-mail Messages

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 requirements are provided in 32 Code of Federal Regulations (CFR) 2001.23 (see Example 5-1).

The following markings are included;

- 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,
- Portion marking of Title or Subject markings (regardless of category), and
- Classification authority block, including the name and title of the classifier, classification authority; and for NSI only, declassification instructions.

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

Examples of electronic files that are marked include, but are not limited to;

- Word processing, database, spreadsheet, and HTML documents,
- E-mail and 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). and

- Because electronic e-mail documents are marked as final, the interior pages are marked accordingly.

Consult 32 CFR Section 2001.23 (Example 5-1) and the Office of Classification Guidelines for Marking Email (Example 5-3) for additional information. 32 CFR 2001 §2001.24 may also be consulted for related 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 may also be created during research or note taking at classified meetings, seminars, classes, symposiums, or conferences. Working papers are:

- 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 as "Working Paper" or "Draft" on the first page of the text,

- Annotated that they may not be used as a classification source when shared with others if they are not portion marked based on appropriate classification authority and contain commingled NSI and RD information (see 32 CFR 2001, § 2001.23 (a)(4) and § 2001.24),

- The appropriate classified cover sheet is used,

- 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 organizational element activity or office,
    - Retained for more than 180 days from the date of origin or less when directed by program requirements, or
    - Filed permanently.

In addition to national requirements for working papers, these documents are marked as "Draft" or "Working paper" on the front cover until they are marked as final documents. RD and FRD drafts and working papers also include the same markings as required for NSI

drafts and working papers. Classification warning information may also be required per 32 CFR 2001, §2001.23(a)(4) and §2001.24(h)(5).

Working Papers or drafts that are frequently updated as part of a project or study, are commonly referred to as "living" documents, and may be considered to be (re)originated upon each change provided the date of each revision, addition, or change is 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 or less when directed by program requirements, without being reviewed for classification and marked as final documents, are considered 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 are either 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 CMCS 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 a draft or working paper is being sent outside the office of origin for a classification review and determination, in addition to the marking described above, it is also marked:

> *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. This document may not be used as a source document for classification.*

If the classification determination cannot be made locally, a Document Undergoing Classification Review cover sheet (see Example 5-2) or similar cover sheet 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 or draft with the highest possible classification level and category.

Notes taken during a meeting, conference, etc. that involve classified information or a classified subject area are to be considered classified working papers and are protected and

marked with the highest potential classification level and category, and with appropriate caveats, as applicable. A review by a DC is conducted if the notes;

- Are removed from the site or facility;
- Become final (a final document),
- Are filed permanently, or
- Are retained longer than 180 days or less when directed by program requirements.

Transmission of notes of uncertain classification is in accordance with Section 11, Receipt and Transmission of Classified Matter.

For more information on marking working papers and drafts, consult the Helpful Websites subsection below.

Points of Contact:

For questions about the CMPC Program, contact your local ODFSA or the Office of Classification at outreach@hq.doe.gov.

Forms/Samples/Graphics:

32 CFR 2001.23 (Example 5-1)

Document Undergoing Classification Review Cover Sheet (Example 5-2)

Guideline for Marking Email on a Classified Network (Example 5-3)

Helpful Websites:

To view the *DOE CMPC Marking Resource*, go to:
http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

To view the *ISOO Marking Classified Information Booklet*, go to:
http://www.archives.gov/isoo/training/marking-booklet.pdf.

EXAMPLE 5-1

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.

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

- Subject to all requirements of the Order.
- 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."
- 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.
- 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.
- 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.

Markings on classified e-mail messages.

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.

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.

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

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.

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.

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.

Marking Web pages with classified content.

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.\

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.

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.

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.

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.

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.

Marking classified URLs. URLs 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

Marking classified dynamic documents and relational databases.

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.

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).

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.

Users developing a document based on query results from a database shall 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.

Marking classified bulletin board postings and blogs.

A blog, an abbreviation of the term "web log," is a Website 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.

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.

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.

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.

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.

Marking classified wikis.

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.

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.

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

Instant messaging, chat, and chat rooms.

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.

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.

Attached files. When 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).

INTENTIONALLY LEFT BLANK

Example 5-2
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

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 cover sheet (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

INTENTIONALLY LEFT BLANK

Example 5-3

Guidelines for Marking Emails
On a Classified Network

Guidelines for
Marking Email
On a Classified Network

U.S. Department of Energy
Office of Quality Management
Office of Classification
Office of Health, Safety and Security

Beta version 1.2

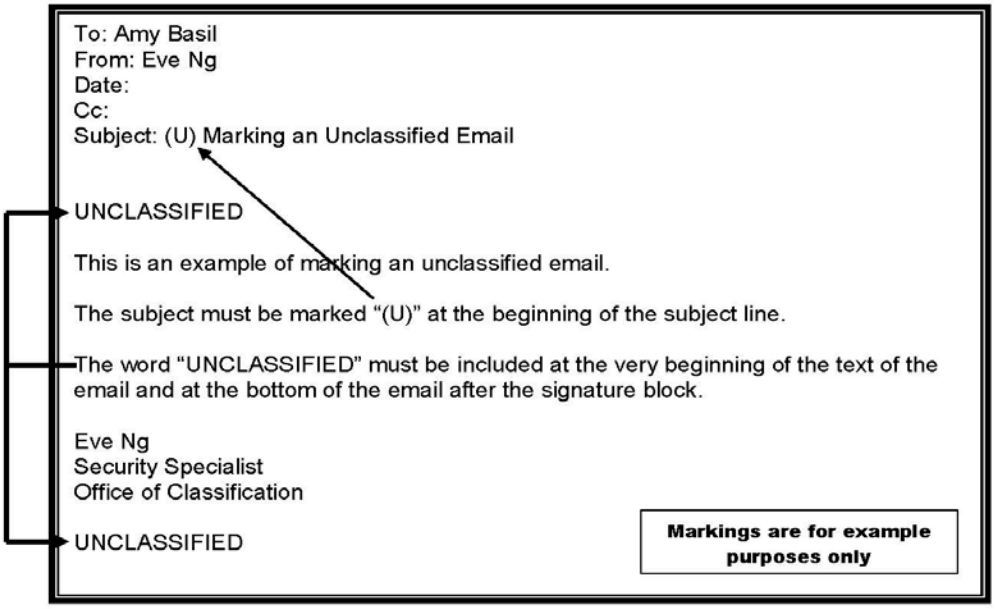
Table of Contents

FOREWORD

This booklet was developed to assist you in marking email generated on a classified network. Each example illustrates the markings required for the types of classified and unclassified information contained in or attached to email and reflects the requirements contained in national and DOE directives. Nothing in this booklet is intended to establish, imply, or mandate requirements. If you have any questions about the contents of this booklet, please contact the Office of Classification at 301-903-7567 or outreach@hq.doe.gov.

4

MARKING EXAMPLE FOR AN EMAIL
CONTAINING UNCLASSIFIED INFORMATION



5

MARKING EXAMPLE FOR A DERIVATIVELY CLASSIFIED EMAIL CONTAINING NATIONAL SECURITY INFORMATION

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Derivatively Classified as NSI

SECRET

(U) This is an example of marking an email that is derivatively classified as containing National Security Information.

(S) The subject line must be marked with the classification level of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level of the email must be included at the beginning of the text of the email and at the bottom after the special control marking.

(C) Since this email contains only NSI, each portion must be marked at its beginning with the highest classification level of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

(U) The special control marking is placed after the classification authority block and before the overall classification level.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: 20280405

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify on: 20280405

Derivative Declassifier review
required prior to declassification

SECRET

Markings are for example purposes only

6

MARKING EXAMPLE FOR AN EMAIL
CONTAINING RESTRICTED DATA INFORMATION

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Classified as RD

SECRET//RESTRICTED DATA

This is an example of marking an email containing Restricted Data information.

The subject line must be marked with the classification level and category (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category (and caveats) of information contained in the overall email. In this example, the subject is unclassified.

The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the RD admonishment marking.

Since this email contains RD information, each portion is not required to be portion marked. If the email is portion marked, the classification level and category (e.g., S//RD) must be indicated for each portion that contains RD.

The 2-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

The RD admonishment marking is placed after the classification authority block and before the overall classification level and category marking.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist, OC
Derived From: CG-XX-1, 9/1/2011, DOE OC

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC

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

Markings are for example purposes only

SECRET//RESTRICTED DATA

7

MARKING EXAMPLE FOR AN EMAIL
CONTAINING FORMERLY RESTRICTED DATA INFORMATION

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Classified as FRD

SECRET//FORMERLY RESTRICTED DATA

This is an example of marking an email containing Formerly Restricted Data information.

The subject line must be marked with the classification level and category (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category (and caveats) of information contained in the overall email. In this example, the subject is unclassified.

The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the FRD admonishment marking.

Since this email contains FRD information, each portion is not required to be portion marked. If the email is portion marked, the classification level and category (e.g., S//FRD) must be indicated for each portion that contains FRD.

The 2-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

The FRD admonishment marking is placed after the classification authority block and before the overall classification level and category marking.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist, OC
Derived From: CG-XX-1, 9/1/2011, DOE OC

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act of 1954.

SECRET// FORMERLY RESTRICTED DATA

Markings are for example purposes only

8

MARKING EXAMPLE FOR A PORTION-MARKED EMAIL CONTAINING RESTRICTED DATA (OR FORMERLY RESTRICTED DATA) AND NATIONALSECURITY INFORMATION

NOTE: An email containing RD or FRD and NSI that is not portion-marked is marked following the example for an email containing only RD or FRD, as appropriate.

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking a Portion-Marked Email Containing RD or FRD and NSI

SECRET//RESTRICTED DATA

(U) This is an example of marking a portion-marked email containing Restricted Data or Formerly Restricted Data and National Security Information.

(S//RD) The subject line must be marked with the classification level and category if RD or FRD (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the source list.

(C) Since the originator decided to portion mark this email, each portion must be marked at its beginning with the highest classification level and category if RD or FRD (and caveats) of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information, which for an email commingling RD or FRD and NSI has special rules. This marking can be in block or linear form.

(C/RD) The RD admonishment marking is placed after the classification authority block and before the source list

(C//RD) The source list containing the declassification instructions with the longest duration for each NSI source is placed immediately before the overall classification level and category marking at the bottom of the email.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist, OC
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: N/A for RD portions; see source list for NSI portions

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A for RD portions; see source list for NSI portions

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

Source List: CG-XX-1, 9/1/2011, DOE OC; Declassify On: 20201025

SECRET//RESTRICTED DATA

Markings are for example purposes only

9

MARKING EXAMPLE FOR AN EMAIL CONTAINING ONLY TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Classified as TFNI

SECRET//TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

(C//TFNI) This is an example of marking an email containing Transclassified Foreign Nuclear Information.

(U) The subject line must be marked with the classification level and category of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(C//TFNI) The overall classification level and category of the email must be included at the beginning of the text of the email and at the bottom after the classification authority block.

(U) Since this email contains TFNI but not RD or FRD, each portion of the email must be marked at its beginning with the highest classification level and category of the information contained in that portion.

(S//TFNI) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist, OC
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: N/A to TFNI portions

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A to TFNI portions

SECRET//TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

Markings are for example purposes only

10

MARKING EXAMPLE FOR AN EMAIL CONTAINING NATIONAL SECURITY INFORMATION AND TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking a Portion-Marked Email Containing NSI AND TFNI

SECRET//TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

(U) This is an example of marking a portion-marked email containing National Security Information and Transclassified Foreign Nuclear Information.

(S//TFNI) The subject line must be marked with the classification level and category if TFNI of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(S//TFNI) The overall classification level and category of the email must be included at the beginning of the text of the EMAIL and at the bottom after the source list.

(C) Since this email contains both NSI and TFNI but no RD or FRD, each portion of the email must be marked at its beginning with the highest classification level and category of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information, which for an email commingling NSI and TFNI has special rules. This marking can be in block or linear form.

(U) The special control marking is placed after the classification authority block.

(C) The source list containing the declassification instructions with the longest duration for each NSI source is placed immediately before the overall classification level and category marking.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist, OC
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: N/A for TFNI portions; see source list for NSI portions

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A for TFNI portions; see source list for NSI portions

Derivative Declassifier review
required prior to declassification

Source List: CG-XX-1, 9/1/2011, DOE OC; Declassify On: 20201025

SECRET//TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

Markings are for example purposes only

11

MARKING EXAMPLE FOR AN EMAIL CLASSIFIED USING MULTIPLE SOURCES

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Classified using Multiple Sources

SECRET

(U) This is an example of marking an email that was classified using multiple sources.

(S) The subject line must be marked with the classification level (and category, if RD or FRD) of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level (and category if RD or FRD) of the email must be included at the beginning of the text of the email and at the bottom after the source list.

(C) Since this email contains only NSI, each portion of the document must be marked at its beginning with the highest classification level of the information contained in that portion.

(U) The appropriate classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

(U) When the classification of an email is based on multiple sources, the entry for the "Derived From" line of the classification authority block is "Multiple Sources." For an email containing only NSI like this one, the entry on the "Declassify On" line reflects the longest duration of classification from all these sources.

(U) Since this email contains only NSI, the special control marking is placed after the classification authority block.

(U) A list of the source documents must be placed at the bottom of the email immediately before the overall classification level (and category if RD or FRD).

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist
Derived From: Multiple Sources
Declassify On: 20280405

Derivative Declassifier review
required prior to declassification

Source Document List:
CG-XX-1, 9/10/10, DOE OC
CG-ZZ-3, 11/12/12, DOE OC

SECRET

Markings are for example purposes only

12

MARKING EXAMPLE FOR A CLASSIFIED EMAIL TRANSMITTING A CLASSIFIED ATTACHMENT

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Email Classified as NSI with an SRD Attachment

SECRET//RESTRICTED DATA

Attachment contains SECRET//RESTRICTED DATA
When separated from attachment, this email is SECRET.

(U) This is an example of marking an email that contains NSI with an RD attachment.

(U) The subject line must be marked with the classification level (and category if RD or FRD) of the information contained in the subject line, not the classification level of information contained in the overall email or attachment. In this example, the subject is unclassified.

(U) The overall classification level (and category if RD or FRD) of the email itself and its attachments must be included at the beginning of the text and at the bottom of the email. Immediately following the overall classification level (and category if RD or FRD) at the beginning of the text, the highest level (and category if RD or FRD) of the attachment must be identified.

(U) Wherever the attachment is shown (at the bottom of the email, elsewhere in the email, or in the attachment line), the classification level (and category if RD or FRD) of the information contained in the attachment must be indicated (e.g., SRD Attachment).

(U) The attachment must be marked correctly as a stand-alone document.

(S) Since this email is classified as NSI, it is portion marked, the 3-line classification authority block is used, and the special control marking is placed after the classification authority block. The "Derived From" line must include the sources used to classify the email. The "Declassify On" line should contain the declassification instruction for the email.

Eve Ng
Security Specialist
Office of Classification

Classified By: Eve Ng, Security Specialist
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: 20280101

Derivative Declassifier review
required prior to declassification

SECRET//RESTRICTED DATA

SRD Attachment

Markings are for example purposes only

13

MARKING EXAMPLE FOR AN UNCLASSIFIED EMAIL TRANSMITTING A CLASSIFIED ATTACHMENT

To: Amy Basil
From: Eve Ng
Date:
Cc:
Subject: (U) Marking an Unclassified Email with a Classified Attachment

SECRET

Attachment contains SECRET
When separated from attachment, this email is unclassified.

This is an example of marking an email that contains only unclassified information but transmits a classified attachment.

The subject line must be marked with the classification level and category of the information contained in the subject line, not the classification level and category of information contained in the overall email or attachment. In this example, the subject is unclassified.

The overall classification level (and category if RD or FRD) of the email itself and its attachments must be included at the beginning of the text and at the bottom of the email. Immediately following the overall classification level (and category if RD or FRD) at the beginning of the text, the highest level (and category) of the attachment(s) must be identified and followed by this statement: "When separated from attachment, this email is unclassified."

Wherever the attachment is shown (at the bottom of the email, elsewhere in the email, or in the attachment line), the classification level (and category if RD or FRD) of the information contained in the attachment must be indicated (e.g., SRD Attachment).

The attachment must be marked correctly as a stand-alone NSI document.

Since this email is unclassified, it is not portion marked and needs no classification authority block.

Eve Ng
Security Specialist
Office of Classification

SECRET

Secret
Attachment

Markings are for example purposes only

14

MARKING EXAMPLE FOR A STRING OF CLASSIFIED EMAIL

To: Eve Ng
From: Amy Basil
Date: Friday, May 24, 2013 10:16 AM
Subject: Re: (U) Marking a String of Emails

SECRET

(U) If you respond to or forward a classified email, you must review and classify the entire string, considering each section in the context of the entire email for classification.

(S) The overall classification level (and category if RD or FRD) of the string is included at the beginning of the text of your email and at the end of the entire string of emails. In this example, the first email is Confidential and the second is Secret; so the string has an overall classification level of Secret.

(C) The classification authority block is placed at the end of the string just before the overall classification level (and category if RD or FRD).

(C) Do not repeat the special control marking or any RD/FRD admonishment for your reply. However, you must carry forward any statements concerning classified attachments to the email string (e.g., "Attachment contains SECRET", When separated from attachment, this email is..." This should be placed at the top of the email string and below the overall classification level (and category if RD or FRD).

(U) For your classification authority block, the "Derived From" line should include all sources used to classify the entire email string. At a minimum, this should include any guide used to make your classification determination and any of the previous email. If a source from the previous email is used, this may be noted with "and email above". If there is a source list, it should be included at the end of the email string above the overall classification. The "Declassify On" line must **reflect the longest duration of classification from all the sources** for the entire string.

Amy Basil
Security Specialist

SECRET

To: Basil, Amy
From: Ng, Eve (HS)
Date: Thursday, May 23, 2013 4:44 PM
Subject: (U) Marking a String of Emails

CONFIDENTIAL

(C) The initial email is marked according to the classification of the information contained in the email. This email contains Confidential NSI.

Classified By: Eve Ng, Security Specialist
Derived From: CG-XX-1, 9/1/2011, DOE OC
Declassify On: 20280405

Derivative Declassifier review
required prior to declassification

CONFIDENTIAL

Classified By: Amy Basil, Security Specialist, HS-61
Derived From: CG-YY-1, 9/1/2011; DOE OC and email above
Declassify On: 20280405

SECRET

Markings are for example purposes only

APPENDIX A
TEMPLATES OF REQUIRED MARKINGS

RD Admonishment:

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

FRD Admonishment:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative
and criminal sanctions. Handle as RESTRICTED
DATA in foreign dissemination. Section 144b, Atomic
Energy Act of 1954.

NSI/TFNI/Commingled Derivative Classification Authority Block:

Classified By:
Derived From:
Declassify On:

NSI/Commingled Original Classification Authority Block:

Classified By:
Reason:
Declassify On:

RD/FRD Derivative Classification Authority Block:

Classified By:
Derived From:

NSI Special Control Marking:

Derivative Declassifier review
required prior to declassification

APPENDIX B
MARKING EXAMPLE FOR AN ORIGINALLY CLASSIFIED EMAIL CONTAINING NSI

NOTE: This example is included for completeness. Original classification should only be done by a Federal employee with original classification authority whose training is up to date.

To: Eve Ng
From: John Sobieski
Date:
Cc:
Subject: (U) Marking an Email Originally Classified as NSI

SECRET

(U) This is an example of marking an email containing information considered to be National Security Information that is not adequately covered by existing guidance. Only an Original Classifier may do this initial classification. Remember that Restricted Data, Transclassified Foreign Nuclear Information, and Formerly Restricted Data are NEVER initially classified by an Original Classifier.

(S) The subject line must be marked with the classification level of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level of the email must be included at the beginning of the text of the email and at the bottom after the special control marking.

(C) Since this email contains only NSI, each portion must be marked at its beginning with the highest classification level of the information contained in that portion.

(C) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form. Rather than listing a guide that the decision is derived from, Original Classifiers must give the "Reason" for classification found in Section 1.4 of Executive Order 13526. This section describes the types of information that may be originally classified.

(S) Another difference is that an Original Classifier must establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Generally, this is 10 years from the date of the original decision unless the sensitivity of the information requires that it be classified for up to 25 years from the date of the original decision.

(C) The "Classified By" line may contain the Original Classifier's name and position OR his/her personal identifier.

(U) The special control marking is placed after the classification authority block and before the overall classification level.

John Sobieski
Director, Examples Division
Office of Classification

Classified By: John Sobieski, Director, Examples Division, OC **OR** ID# 55500
Reason: 1.4(c)
Declassify On: 20240202

OR

Classified By: John Sobieski, Director, Examples Division, OC Reason: 1.4(c); Declassify On: 20240202

Derivative Declassifier review
required prior to declassification

Markings are for example purposes only

SECRET

Section 6

Protection of Classified Matter in Use

This section addresses DOE procedures pertaining to the protection of classified matter while it is in use. When it is not actually being used, it is stored within a security container, vault, or vault type room (VTR) that is approved for open storage of classified matter, or in approved non-conforming storage. (See Section 7, Storage of Classified Matter).

Implementation Guidance:

All persons who are authorized to access classified matter possess the appropriate security clearance or access authorization 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 is protected at all times and, as a general rule, will be accessed for use only in approved Limited Areas (LA) or higher security areas. Classified matter that is not in use is in approved storage.

Emergency Situations:

If an 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 are taken after the emergency;

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

Fire and Evacuation Drills:

Fire and evacuation drills should 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 are 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 is limited to the minimum required to achieve the intended purpose,

- The information is transmitted over approved U.S. Government channels using the most secure and expeditious method deemed necessary when time is of the essence,

- The recipient is informed of what specific information is classified and the protection requirements for the information,

- The recipient is briefed on his/her responsibilities for not disclosing the information and signs a nondisclosure agreement. When time does not allow for this to be done prior to access, it is done as soon as possible following access, and

- The amount of classified information disclosed remains at the absolute minimum necessary to achieve the purpose it was provided.

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 reports the disclosure. That report includes:

- 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, and

- How the information is being protected.

The disclosure report is made to:

- The Associate Under Secretary for Environment, Health, Safety and Security, AU-1; the NNSA Associate Administrator for Defense Nuclear Security (NA-70); and the ODFSA when RD or FRD has been released, and

- The ODFSA 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, contact the ODFSA or e-mail the Office of Security Policy at: Security.Directives@hq.doe.gov.

INTENTIONALLY LEFT BLANK

Section 7
Storage of Classified Matter

This section addresses DOE procedures pertaining to the storage of classified matter. In summary, all classified matter is stored within a security container in an LA or higher security area, or other security area approved for open storage of classified matter.

Implementation Guidance:

Classified matter is stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment or security areas whenever it is not under the direct control of an authorized person.

Requirements for Intrusion Detection Systems (IDS) that are used for supplemental control are established in DOE physical protection directives.

Requirements for vaults and Vault Type Rooms (VTRs) used for open storage of classified matter are established in DOE physical protection directives.

Storage Containers:

- Storage containers used to store classified matter are not used to store or contain other items that may be a substantial target for theft;
- Storage containers used for storing classified matter conform to current U.S. General Services Administration (GSA) standards and specifications;
- Combinations are set by an appropriately cleared and authorized individual;
- Combinations are changed as soon as practical whenever a current combination may be known by someone who does not possess the requisite access authorization, formal access approvals, and need to know for all of the information stored in the container;
- A record is maintained of each individual who has been granted access to any secure storage repository combination;
- SF 700 Parts 1, 2, and 2A are completed for each secure storage repository or other location approved for storing classified matter that uses a combination;
    - The combination is available for authorized use,
    - The local implementation plan may dictate whether Block 8, Serial Number of Lock, should be left blank,

  - SF 700 Part 1 is affixed to the inside of the door of vaults and VTRs containing the combination lock. For security containers, it is placed inside the locking drawer,

- An SF-702 is used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who has opened, closed, or checked a particular container, room, vault, or VTR holding classified information;

- No signage indicating that classified information is stored in the security container or repository may be posted on the exterior of the container or repository.

Top Secret matter is stored in one of the following three ways.

- In a locked, GSA-approved security container with one of the following supplemental controls:

  - Under IDS protection and by protective force (PF) personnel responding within 15 minutes of alarm annunciation; or
  - Inspections by PF personnel no less frequently than every 2 hours.

- In a locked vault or VTR within a limited area (LA), protected area (PA), or material access area. The vault or VTR is equipped with IDS equipment, and PF personnel respond within 15 minutes of alarm annunciation.

- In a locked vault or VTR within a property protection area or outside of a security area, and under IDS protection. PF personnel respond within 5 minutes of alarm annunciation.

Secret matter is stored:

- In any manner authorized for Top Secret matter;

- In a locked vault or in a locked GSA-approved security container within an LA or higher security area; or

- In a locked VTR with the following supplemental controls:

  - Inspections by PF personnel no less frequently than every 4 hours; or
  - For a VTR located within a PA or higher security area, the PF personnel respond within 30 minutes of the VTR's IDS alarm.

- When stored in a locked GSA approved security container inside a Property Protection Area (PPA) or outside a security area, all classified matter is in formal accountability.

Confidential matter is stored in the same manner prescribed for Secret or Top Secret matter; however, the supplemental controls are not required.

Nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material is stored in a vault or VTR located in an LA or higher security area, with;

- IDS supplemental control, and

- PF personnel respond within 15 minutes of the IDS alarm,

PF personnel, private security firms, or local law enforcement agency personnel respond to IDS alarms as specified and documented in the local security plan.

Nonconforming storage may only be used for classified matter that cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, nonconforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

- Nonconforming storage results in protection effectiveness equivalent to that provided to similar levels and categories of classified matter by standard configurations.

- The methods, protection measures, and procedures are documented and approved by the ODFSA.

- Documentation includes the following,

    - An explanation as to why exercising this option is necessary,
    - A description of the classified matter to be stored,
    - An analysis demonstrating the means by which equivalent security is to be provided, and
    - Copies of the documentation are forwarded to the cognizant HQ program office.

Permanent burial is an option that may be approved by the ODFSA for permanent placement of classified matter. Permanent placement is not a form of destruction for classified matter. In addition to meeting the requirements for nonconforming storage of classified matter, permanent burial documentation also includes:

- For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial;

- Configuration of classified matter to be buried;

- Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter; and

- Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter.

Accountable classified matter is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.

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 (under the direct supervision of authorized persons). These individuals 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 by the ODFSA).

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 XO series combination door lock, check the life-safety switch; 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 is 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 XO 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.

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

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

  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.

  NOTE 3: Facilities are required to utilize the XO series combination locks on security containers.

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 are 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: Premise alarms for VTRs, when so equipped, are activated whenever the facility is unoccupied.*

- Record each closing/checking action on the SF-702, which is 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 local ODSA, ODFSA, protective force (PF) 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 notifies another cleared individual or protective force officer who in turn, follow the plan of action detailed in the local security plan. The discovery is also reported to the ODFSA or custodian responsible for the LA or VTR so they can report the discovery as a security incident. The area remains protected, and every effort is made to leave the area untouched or undisturbed until a decision to proceed has been granted according to the procedures in the local security plan. Appropriately cleared management or other cleared personnel stand by the area until the potentially compromised classified matter is secured or until released as documented in the local security plan. The individual discovering the forced entry stands by until he or she has given a statement to the PF officer or ODFSA. A complete inventory of the contents of the protected matter is made as soon as the scene has been released.

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 notifies another cleared individual or PF officer, who in turn, follows the plan of action detailed in the local security plan. The PF officer 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 ODFSA.

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 officer to relock the container. The person notified or another individual responsible for the container inventories the contents of the container no later than the next working day.

The ODFSA or other authorized cleared individual will initiate action to change the combination, which is considered potentially compromised, as soon as possible during duty hours or after the start of the next work day, 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 is assumed and management is immediately informed via secure communication.

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

Security container combinations (SF-700s) of other security containers stored within a container that has been found open and unattended may have to be changed. An Incident of Security Concern inquiry is initiated whenever a security container is found open and unattended and any stored SF-700 combination envelopes in the security container are examined for tampering. An expanded inquiry is 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 assumes 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 notifies their ODFSA 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 is generated and the combination may need to be changed, as described above.

(See Section 15, Incidents of Security Concern for additional information on this topic.)

Controlling Access to Security Repositories:

Individuals requiring access to a security container or VTR have the appropriate security clearance or access authorization, special accesses for the highest classification level and most restrictive category, as well as any caveat requirements and need-to-know for the information stored in that repository. For example, only individuals with a "Q" access authorization 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" access authorization 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 are secured when an individual with the appropriate security clearance or access authorization and need-to-know does not have visual line-of-sight to the front of the container.

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

A security container with a combination lock on each drawer (multi-lock security container) has a separate classified combination for each drawer, each one with a separate SF-700. A multi-lock security container 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 security containers are generally used for compartmentation purposes. If an SF-702 is used for each drawer, the combination lock on each drawer is checked at the close of each business day the container may have been accessed.

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," 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 is stored in separate containers unless programmatic requirements dictate otherwise.

Access to NATO documents requires an access briefing administered by the National Nuclear Security Administration Office of Resource Management and Mission Support (NA-72), which performs NATO Subregistry functions for DOE. Documents are segregated from other documents when stored in security containers. At a minimum, NATO documents may be segregated by being placed in separate files. If NATO documents are stored in a container with other classified documents, access to the container itself is 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 is 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.

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

End-Of-Day Security Check:

An SF-701, *Activity Security Checklist* (or equivalent form) is used for end-of-day security checks of VTRs, and other areas (such as Limited Areas) that contain security interests (e.g., security repository, classified computer, classified shredder, etc.). These forms should be maintained **inside** each VTR or area containing security interests. The form is 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 IDS protection and XO-series combination locks on the door. Open storage approvals and certificates are granted before open storage is implemented.

Individuals who access these areas possess the appropriate security clearance or access authorization for the highest classification level and most restrictive category of information that is in open storage as well as a need-to-know for official duties.

Individuals without the appropriate security clearance or access authorization and need-to-know are escorted by a person with the appropriate security clearance or access authorization and need-to-know while they are in the area. The escort announces to others that an uncleared individual or individual without the need-to-know, proper clearance and/or authorization is in the area and ensures that the individual they are escorting is not given access to information to which they are not authorized.

All classified matter exceeding the clearance level or access authorization of the person to be escorted, including such items as classified equipment and/or classified maps, photographs, and charts on walls, are 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, sign in on a visitor log, which contains their printed name, signature, date, time in, time out, and name of escort. The only exception is when entering personnel are restricted from access to special nuclear material (SNM) or classified matter (e.g., a foyer-type area), logging entry and exit is not required. Visitor logs for these approved areas are retained for 5 years. Visitor logs may be locally produced.

Access control, whether by mechanical means, electromechanical means, or personnel, are 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 Information:

An SF-702 is 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 are 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 contains at least one daily duty-day entry that the container was “checked by” with time and initials, at the close of each day the repository or container may have been accessed. PF checks, when required, are in addition to this check. Each container opening and closing is 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." ODFSAs or their designees develop local procedures to ensure that all classified matter is properly stored and that security containers are checked at the end of each work day.

SF-702s are 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 ODFSA, for guidance.

Security Repository (Safes and Doors) Combination Information:

Combinations to security containers, authorized open storage area combination-locked security access doors, and VTRs are 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 or access authorization 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 is handled as a security incident and reported via secure channels.

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

NOTE 2: The name and signature of the cleared individual changing a combination is 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*** *always required. The risk of lockout and damage to the XO-series lock outweighing any gained advantage of extracting the serial number is determined by the ODFSA.*

NOTE 4: Top Secret combinations are brought into accountability.

NOTE 5: Combinations to containers storing accountable NATO classified information are 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, are also listed, but addresses and phone numbers are not required. Additional cleared personnel are added to this record when they receive the combination.

NOTE: There is 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 is then 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 is 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. ODFSAs or their designees should determine the storage locations for such SF-700s by organizational element or sub-element. Combinations protecting Sensitive Compartmented Information (SCI) are stored within a Sensitive Compartmented Information Facility (SCIF). An SF-700 containing a TS combination are appropriately stored and brought into accountability. The creation of a "master combination list" of multiple combinations for any program, office, or organizational 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 Central Alarm Station (CAS) or other location specified in the local security plan for storage. For purposes of life safety and emergency response, this ensures that the protective force or other authorized individual(s) 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):

Custodians, an ODFSA, or their designee are 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 ODFSA coordinates with the local Accountable Property Representative (APR) to

ensure that the safe is empty, the combination is reset, and the movement is completed. The ODFSA or their designee is responsible for removing the safe from his or her classified repository listing in the local security plan. Detailed instructions for turning in a safe are included in Example 7-1.

2. The safe is being relocated to another room with no change in custodians. In this case, the ODFSA or their designee coordinates with the local APR to ensure that the safe is configured for movement and that the movement is completed. The ODFSA is responsible for updating his or her classified repository listing in the local security plan to show the new location of the safe. Detailed instructions for relocating a safe with no change in custodians are included in Example 7-2.

3. The safe is being transferred to another custodian. In this case, the ODFSA coordinates with the local APR to ensure that the safe is configured for movement and that the movement is completed. The ODFSA is responsible for updating his or her classified repository listing in the local security plan to show the new location and custodian of the safe. Detailed instructions for relocating a safe with a change in custodians are included in Example 7-3.

NOTE: Relocating a security container or rearranging furniture within an alarmed room may interfere with the electronic protective system. Therefore, the ODFSA or other Survey Team personnel 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 (OF) 89 is 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 remains 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 is entered and signed on the OF 89 by the technician and, or if required, the 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 is removed and a permanent sign affixed to the front stating "Not Authorized for Classified Storage."

24-Hour Classified Receipt and Storage:

Procedures are established for circumstances in which any person who has possession of classified matter up to TS/RD (not including SCI and Special Access Program (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 location authorized in the local security plan. The location(s) and the procedures to be followed are approved by the ODFSA and employees are trained on the process.

Procedures include reporting requirements which include, at a minimum, notification of the ODFSA no later than the following business day.

Points of Contact:

For the names and contact information for those who occupy the positions identified in this section, contact your local ODFSA.

Forms/Samples/Graphics:

How to Excess a Safe (see Example 7-1).

Moving a Safe with No Change in Custodians (see Example 7-2).

Moving a Safe with a Change in Custodians (see Example 7-3).

OF 89, *Maintenance Record for Security Containers/Vault Doors Federal Standard* (for a copy of this form go to: http://www.gsa.gov/portal/forms/download/115434).

SF-700, *Security Container Information* (for information on obtaining this form go to: http://www.gsa.gov/portal/forms/download/115574).

SF-701, *Activity Security Checklist* (for a copy of this form go to: http://www.gsa.gov/portal/forms/download/115578).

SF-702, *Security Container Check Sheet,* (for a copy of this form go to: http://www.gsa.gov/portal/forms/download/115582).

HQ F 5632.12, *Container Equipment Inspection Certificate* (see Example 7-1).

Helpful Websites:

To view the *DOE CMPC Marking Resource*, go to: http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource.

INTENTIONALLY LEFT BLANK

EXAMPLE 7-1

How to Excess a Safe

- Before disposing of a safe, contact your local ODFSA so that he or she can guide you through the steps of preparation. For instance, if your safe is broken (it will not unlock, the handle will not turn, or a drawer is stuck), your ODFSA may have to have it drilled before you can access it to check for classified material.

- The ODFSA should then contact the APR within his/her organizational element and request that the safe be turned in as excess. The APR, in turn, arranges a date and time to move the safe. The ODFSA should then inform you of that date/time.

- The ODFSA should also make an appointment to have the combination on the safe reset to its factory setting (50-25-50).

- **BEFORE** the move date of your safe, you and your ODFSA or their designee should:

  1. Examine the security container, remove all contents, and either destroy the classified contents or store them in another security container (instructions on this process are listed below under "Forms to be Used").

  2. Destroy both the current SF-700, *Security Container Information*, that is inside the safe and the extra copy that should be stored elsewhere (it contains the actual combination to your safe). The SF-700 should be destroyed as appropriate for its classification level.

  3. Attach a handwritten sign on the front of the safe stating "EMPTY." (This is optional, but it is recommended because it clearly indicates that the safe has been cleared out.)

  4. You and your ODFSA or their designee should be present when the task of resetting the combination is completed (i.e., ensuring that it has been set back to the factory setting).

  5. Finally, complete and affix HQ F 5632.12, *Container/Equipment Inspection Certificate* (see form listed below) or equivalent form, ensuring that the safe is empty and ready to be moved. The safe should not be moved if the form is not attached.

After the safe is turned in, the ODFSA or their designee removes the safe information from their classified repository listing in the local security plan.

Your ODFSA will provide the forms and instructions that you need for the excess process.

Listed below is a sample form, Standard Form, and Optional Form you will need before excessing your safe container and instructions on where to find them.

Forms Used when Excessing a Safe or Transferring to New Custodian

HQ Form 5632.12, Container/Equipment Inspection Certificate

This form is an example of the form used at DOE HQ. This form or one similar is completed and signed by the owner of the safe **and** the ODFSA. Before the form is completed, the owner of the safe should check each of its drawers to ensure that no classified matter and/or documents remain. The owner should use a flashlight to check the very back of and underneath each drawer to verify that no documents are "stuck" in between or under the drawers. Any items in the safe at the time of inspection are removed and, if classified, stored properly in another security container, or destroyed. The ODFSA or their designee should be present to witness the owner's inspection of the safe and ensure that the inspection is complete (signing the inspection sheet). The form should then be taped to the front of the security container.

Standard Form 700, *Security Container Information*

This form is inside every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form contains information about the safe, its custodian(s), information on who to contact in case the safe is found open and unattended, and the names of all personnel with access to the safe. The cover sheet (Part 1) of the form and all copies of the combination portion (Parts 2 and 2A) of the form should be destroyed when the safe is turned in as excess. The form should be destroyed consistent with the classification level and category shown on it.

When transferring to a new custodian, the safe's new owner creates a new SF-700 and posts it properly within each locking drawer. The combination portion of the SF-700 is placed in a different security container and at the location listed in the local security plan.

Optional Form 89, Maintenance Record for Security Containers/VTR Doors

This form is in every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form is usually blank but will be completed when and if the security container requires maintenance of any kind. ***This form should ALWAYS remain inside the security container,*** *whether it is moved or not. This form can be found here: http://www.gsa.gov/portal/forms/download/115434. You can print the form and put it in your security container.*

At the end of this process, nothing should remain in the security container except the OF 89.

DOE F 5632.12, CONTAINER/EQUIPMENT INSPECTION CERTIFICATE

PUT TAPE ACROSS HERE

№ 1012

HQ F 5632.12
(02-90)
Replaces HQ F 5632.1

CONTAINER/EQUIPMENT INSPECTION CERTIFICATE № 1012

INSTRUCTIONS FOR RELEASING ELEMENTS

1. Search container/equipment thoroughly and remove all material. Remove and check under each drawer, leaf or part which might conceal material. CONTACT YOUR SECURITY COORDINATOR IF YOU NEED ASSISTANCE.
2. Lockable containers must be unlocked with key taped inside.
3. Combination locks must be set at 50-25-50.
4. Complete one copy of this certificate. If you are inspecting a desk, tape certificate to underside of top center drawer. Tape the certificate to the back of other containers or equipment.
5. Request pick-up of container/equipment. Do not abandon.

TYPE CONTAINER/EQUIPMENT ☐ Cabinet ☐ Desk ☐ Safe ☐ Other *(Specify)*	SERIAL NO:	DOE NO:

I CERTIFY THAT I HAVE INSPECTED AND REMOVED ALL MATERIAL

NAME *(type or print)*	SIGNATURE	ORGANIZATION	DATE

I CERTIFY THAT THIS CONTAINER/EQUIPMENT CONTAINS NO CLASSIFIED MATERIAL

NAME *(Chief, releasing element)*	SIGNATURE	ORGANIZATION	DATE

INSTRUCTIONS FOR PROPERTY & SUPPLY (P&S) REPRESENTATIVE

1. Search container/equipment thoroughly. Remove and check under each drawer, leaf or part which might conceal material.
2. If any classified material is found, notify the physical Security Branch.
3. Complete lower portion of this certificate. Detach along perforated line, leaving numbered portion taped to container/equipment.
4. Forward lower portion to Physical Security Branch for retention.

I CERTIFY THAT I CHECKED THIS CONTAINER/EQUIPMENT AND THAT IT CONTAINS NO CLASSIFIED MATERIAL

NAME *(P&S Rep) (Print)*	SIGNATURE	ORGANIZATION/OFFICE ROUTING SYMBOL	DATE

U.S. DEPARTMENT OF ENERGY

EXAMPLE 7-2

Moving a Safe with No Change in Custodians

- Before moving any safe from one location to another, i.e., a different office location, contact your ODFSA for specific instructions.

- If you are moving the safe because you are relocating to another office, determine whether any other individuals who currently share your safe or have access to the combination should continue to remain on your SF-700.

- Your ODFSA will contact your local APR who, in turn, requests a date for the safe to be moved. The APR will notify you when this date is established.

- If you are to remain the custodian for the safe, you do not have to check or empty the contents, complete any forms, or change the combination. You should, however, change the room number on your present SF-700, *Security Container Information* (all copies).

- If you are moving the safe because you are relocating to another office, whether any other individuals who currently share your safe (i.e., who have access to the combination) should remain on your SF-700. If you do not want those persons to have access to your safe in your new location, complete a new SF-700 showing you as the custodian and any other individuals that you choose to have access to your safe.

- The safe remains locked at all times during the move.

- It is advisable that either you or your ODFSA or their designee be present during the move to ensure that there is no compromise of the safe or its contents and that the safe is delivered to its designated location.

No additional forms are needed for this particular move situation. However***, the ODFSA should change their classified repository listing in the local security plan to reflect the new location of the safe. It is also a good practice for the ODFSA or their designee to advise the APR of the fact that the safe has been moved and provide the old room number and the new room number, so that the APR can update the property records.***

INTENTIONALLY LEFT BLANK

EXAMPLE 7-3

Moving a Safe with a Change in Custodians

- Before moving a safe from one location to another, i.e., a different office location, contact your ODFSA for specific instructions.

- Your ODFSA or their designee will contact your local APR to request a change in ownership of the safe and to schedule a date for moving it. The APR, in turn, should request a date for the safe to be moved. The APR will notify you when this date is established.

- The ODFSA or their designee will make an appointment to have the combination on the safe reset to a number of the new custodian's choosing.

- **BEFORE** the transfer/move date of the safe, you and your ODFSA or their designee should:

    1. Examine the safe, remove all contents not required by the new Custodian and either destroy the classified contents or store them in another security container. (Instructions on this process are listed below under "Forms to be Used"). All OF 89s, *Maintenance Record for Security Containers/VTR Doors*, **are retained within the safe**.

    2. Destroy both the SF-700, *Security Container Information*, that is inside the safe and the extra copy that should be stored elsewhere (it contains the actual combination to your security container). The old SF-700 should be destroyed as appropriate for the classification level of the SF-700.

    3. Attach a handwritten sign on the front of the safe stating "EMPTY." (This is optional, but it is recommended because it clearly indicates that the safe has been cleared out.)

    4. Complete and affix HQ F 5632.12, *Container/Equipment Inspection Certificate* (see form listed below) or similar form, ensuring that the safe is empty and ready to be moved. The safe should not be moved if the form is not attached.

    5. The new custodian and their ODFSA or their designee should be present when the task of resetting the combination is completed, ensuring that the new combination is known to the new owner and works properly.

    6. The new custodian completes a new SF-700 with the new combination, new owner information, and information about all those who will have access to the safe.

- **AFTER** the safe is moved, the ODFSA or their designee annotates their classified repository listing in the local security plan to reflect the new owner(s) and location. If the new owner or location is a different organizational element, the ODFSA transferring the safe should contact the ODFSA gaining the safe to advise them of the move. If the move is within the same organizational element, it is also a good practice for the ODFSA to e-mail the APR detailing the fact that the safe has been moved and providing the name of the new custodian and the location, so that the APR can update the property records.

Section 8
Reproducing Classified Matter

This section describes how to properly reproduce classified documents.

Implementation Guidance:

Reproduction of classified documents is limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations indicated on the document. Reproduction is 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;

- Top Secret/Foreign Government Information (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 are destroyed in accordance with Section 14, 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,

  FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY

  REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR.

Reproduced accountable documents are brought into accountability (see Section 9, Classified Matter Accountability).

Reproduction Machines:

Reproduction of classified documents is accomplished only on machines located within limited areas (LAs), vault type rooms (VTRs) or higher security areas that are specifically approved by the

ODFSA for classified reproduction. The LA or VTR location is also accredited for classified reproduction and so annotated on the local security plan.

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 contains the make, model and property number (if any) of the authorized copier and be signed and dated by the local ODFSA and/or Information Systems Security Officer (ISSO). 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 in Example 8-1. Additionally, notices regarding any restrictions or requirements pertaining to the reproduction of classified documents on a particular copier are also posted conspicuously next to the copier. A sample of Classified Reproduction Procedural Instructions to be posted by the ODFSA or their designee is provided in Example 8-2.

All reproduction machines that are within an LA, VTR, or higher security areas but are NOT approved for classified reproduction have a sign posted near the machine indicating it is not approved for classified reproduction. A sample sign is provided in Example 8-3.

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

Both classified and unclassified digital copiers undergo an approval process prior to purchase or lease. The local ISSO can help determine which digital copiers may be acquired and what security measures will be met. Also, the ODFSA or their designee should be informed when a new copier is acquired.

Any digital copier located in an LA accredited for closed storage and for classified reproduction has had its hard drive removed and appropriately stored and is powered down whenever the area is unattended. Likewise, any digital copier located in a VTR that is not approved for open storage is powered down and the hard drive removed and stored as described above. Digital copiers without hard drives may be located in LAs or VTRs accredited for closed storage and classified reproduction; such copiers are still powered down (turned off or unplugged) when the area is unattended.

Digital copiers located in VTRs approved for open storage may be left unattended without removing the hard drive or powering down the machine in accordance with approved open storage procedures.

Reproduction Process:

Inside an LA or VTR, classified documents are transported to and from the reproduction machine area in the appropriate manner (see Section 11, Receipt and Transmission of Classified Matter). Access to classified matter being reproduced is 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 is 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 ODFSA immediately regarding this problem.

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

Classified copies should be properly marked as soon as possible.

Reproducing classified matter is not done on copiers located outside of LAs, VTRs, or higher security areas.

Points of Contact:

For information about reproduction, contact your ODFSA or for policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Sample Classified Reproduction Certification Sign (see Example 8-1)

Sample Classified Reproduction Procedural Instructions Sign (see Example 8-2)

Sample Copier Not Approved for Classified Sign (see Example 8-3)

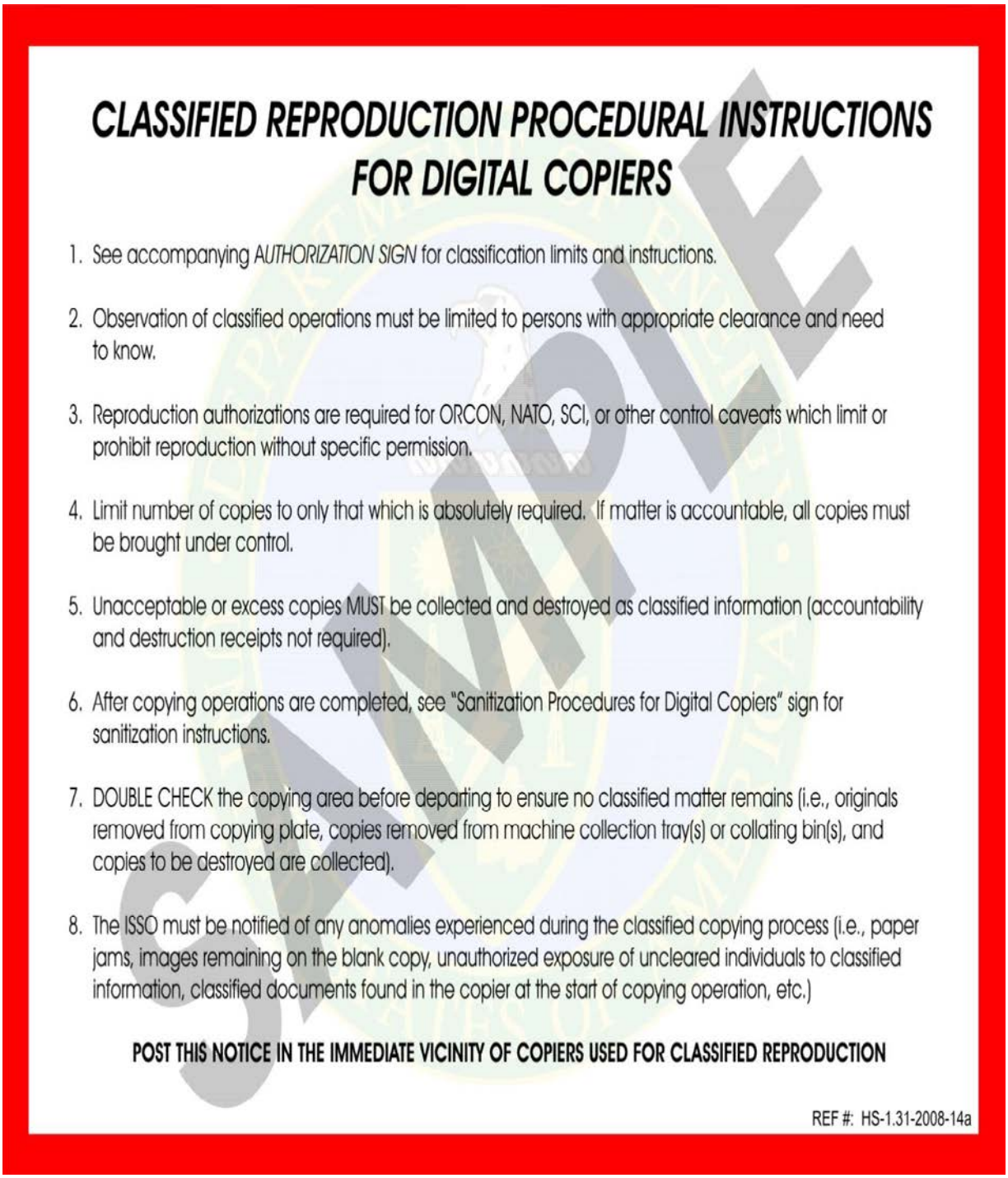
INTENTIONALLY LEFT BLANK

EXAMPLE 8-1

Sample Classified Reproduction Certification Sign

EXAMPLE 8-2

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 persons 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 specific 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 Copiers" 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 ISSO 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 CLASSIFIED REPRODUCTION

REF #: HS-1.31-2008-14a

EXAMPLE 8-3

Sample Copier Not Approved for Classified Sign

INTENTIONALLY LEFT BLANK

Section 9

Classified Matter Accountability

Several types of classified matter 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 Department of Energy (DOE) that are accountable include, but may not be limited to:

- All Top Secret (TS) matter, including TS/Foreign Government Information (FGI);
- Secret/Restricted Data (S/RD) (or higher) matter stored outside a limited area (LA) or higher;
- Any matter that requires accountability because of national, international, or programmatic requirements;
- National requirements, such as Cryptography (CRYPTO) and designated Communications Security (COMSEC) (see CNSSI 2001, CNSSI 2004 and DOE O 470.6, Technical Security Program);
- 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., Special Access Programs (SAP) and Sigma 14);
- Secret documents containing FGI if so designated in a treaty or international agreement; and
- 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 (O) 471.6, Admin Chg 2 *Information Security*. The media formerly designated as ACREM remains 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. The

records of those resulting accountable documents are recorded and maintained as accountable as documented by the process and procedures approved in the local security plan. Due to the fact that the classification is based on the highest classification of the information stored within the security container and the small size of the SF-700, the Classification Authority Block information is not required on an SF-700.

Implementation Guidance:

Accountability Systems:

Classified Matter Control Station (CMCS) personnel within each organizational element, site or facility with the assistance of the ODFSA, establish a system to track accountable classified matter. See Section 10, Classified Matter Control Stations, for a discussion of CMCS operations. Accountability records include information about when accountable matter is originated, reproduced, transmitted, received, destroyed, and/or changed in classification.

Accountable documents are assigned a unique number to track the document throughout its life in that office. The accountability system has 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 O 471.6, Admin Chg 2, *Information Security*.

Inventories:

CMCS personnel inventory all accountable documents, at a minimum, annually. The inventory includes 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 are reported to the ODFSA or their designee who in turn reports those findings as required in the local security plan. Inventory discrepancies may be reportable as Incidents of Security Concern as described in Section 15, Incidents of Security Concern. Completion of a DOE F 5639.2, *Reporting Unaccounted for Documents*, may be required in order to document the inventory discrepancy.

In conjunction with the inventory process, or on a continuous basis, the ODFSA or ODSA ensures that organizational classified holdings are reviewed for documents or other matter that are no longer needed in order to reduce classified holdings.

Accountability Records

Accountability records 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, has a unique number assigned to it);

- Classification level, category (if RD, Formerly Restricted Data (FRD), or Transclassified Foreign Nuclear Information (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; and

- The individual who checked it in and/or out (i.e., the person who has personal responsibility for it).

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 the CMCS procedures in the local security plan (see Section 10, Classified Matter Control Stations).

Accountable information temporarily transferred to another organization within the same facility is entered into the receiving organization's accountability records if the material is kept more than 180 days (or the number of days documented in the local security plan) without return to the sender.

Master files and databases created in central data-processing facilities or information systems to supplement or replace Top Secret records are not authorized for disposal under General Records Schedule 18.

All accountability records (e.g., logs, inventory records, receipts) for Secret and Confidential material are maintained for 2 years. Accountability records for Top Secret are maintained for 5 years.

Points of Contact:

For information about the local Classified Matter Protection and Control (CMPC) Program, contact your ODFSA or for CMPC or other Security policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

DOE F 5639.2, *Reporting Unaccounted for Documents* (for a copy of this form go to http://energy.gov/sites/prod/files/cioprod/documents/5639-2.pdf)

DOE F 1324.5, *Request for Records Disposition Authority* (for a copy of this form go to *http://energy.gov/cio/downloads/doe-f-13245*)

Helpful Websites:

To view DOE O 471.6, Admin Chg 2, *Information Security*, go to: https://PIR.doe.gov

Section 10

Classified Matter Control Stations

Department of Energy (DOE) Order (O) 471.6, Admin Chg 2, *Information Security*, requires that handling and protection procedures be established, documented, and adhered to for classified information throughout its lifecycle (which includes origination, classification, marking, accountability, in-use, storage, reproduction, transmission, and destruction). For purposes of this document, the term Classified Matter Control Station (CMCS) will be used to describe one way to achieve this purpose and to control the classified matter received by and/or dispatched from DOE facilities. Personnel are designated and specially trained to operate these control stations and have the appropriate security clearances or access authorizations and need-to-know commensurate with the level of their classified matter control responsibilities.

Implementation Guidance:

Applicability and Scope --

Each location that receives or transmits classified matter, or that has the potential to receive or transmit classified matter, establishes at least one CMCS. A CMCS is a gateway through which all incoming and outgoing classified matter transits, with the possible exception of e-mails which may or may not be required to be documented through the CMCS until printed based on local procedures. There may be more than one CMCS established when additional CMCSs are needed for efficient operations. Any location that has minimal classified holdings or only an occasional need to receive or transmit classified matter may establish a partnership with another location to use their CMCS. This relationship is documented in the local security plan.

The purpose of the CMCS is to prevent unauthorized access to and unauthorized removal of classified matter. A CMCS is the primary point where classified matter may be received or transmitted by the organizational element, site or facility. CMCS 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 organizational element.

CMCS Standard Operating Procedures are developed in detail and updated as necessary by the station operators in consultation with the local CMCS personnel and the ODFSA or their designee.

Appointments and Designations:

Classified Matter Control Station Operators and Alternates – The Head of each HQ Departmental Element/Program or Field Office with a CMCS, **or their designee**, appoints one Primary CMCS Operator and at least one Alternate CMCS Operator for each CMCS

within the organizational element. The responsible names of the appointees are included in the local security plan (usually as an Appendix). The names of the appointees are readily available for surveys and inspections. The number of CMCS operators should be kept to the minimum required to process the amount of classified mail, facsimiles, and other matter received or transmitted by the organizational element. CMCS personnel possess the appropriate security clearance or access authorization commensurate with the highest level and category of classified matter that passes through the CMCS.

Classified Mailing Address (CMA) Authorized Recipients – Each location with a CMCS may appoint specific cleared individuals who are authorized to receive classified United States Postal Service (USPS) or overnight Express mail. For the purposes of this document, they are called CMA Authorized Recipients; however, there may be other titles used for these individual. These individuals would normally be a CMCS operators; however, in unique circumstances where minimal additional designees are required, other cleared personnel may be appointed. CMA Authorized Recipients who are not CMCS operators are trained in the handling of classified matter in accordance with operational procedures in place within the organization.

Central Mailrooms – The central mailroom for each location only deliver classified mail to a CMCS. They need to be informed of the locations of all CMCSs and the names of any CMA Authorized Recipient who can accept classified mail when it is delivered. The mailrooms receive this information from the ODFSA, ODSA or from a listing in the local security plan.

The ODFSA or ODSA also provide immediate updates to the Central Mailroom and CMCS personnel as required when there are personnel changes.

CMCS Training:

All CMCS personnel complete CMCS training before assuming CMCS duties. This training is tailored to the responsibilities of CMCS personnel and includes the following subject areas: generation and marking, physical protection and storage, reproduction, accountability, transmission and receipting (including hand-carry), destruction of classified information, and emergency procedures. CMCS training is provided as determined by the ODFSA for their site or facility. All CMCS training is documented and the training records retained.

CMCS Operations:

Receipt of Classified Matter – All incoming classified matter transits through an organizational element's CMCS before being released for storage in any other designated classified document repository. This requirement applies to all incoming classified mail, as well as other classified matter hand carried into the site or facilities as provided in the local security plan.

Upon receipt of the matter, CMCS 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 repository custodian. When transferring classified matter to another authorized classified repository custodian or classified matter user within the organization, CMCS personnel are responsible for ensuring that they give the classified matter only to individuals with the appropriate security clearance or access authorization (i.e., a security clearance or access authorization 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).

CMCS personnel 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. CMCS personnel affix the appropriate classified cover sheet to the document (if it is not already affixed). Any other discrepancy in document marking is reconciled between the document recipient and the sender.

CMCS 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 ODFSA is notified. Copies of signed receipts are maintained at the CMCS 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 in all cases, any receipt received with Confidential matter is signed and returned.*

Transmission of Classified Matter – All classified matter being transmitted out of an organizational element serviced by a CMCS, site or facility (mailed or hand carried) is processed through the organizational element's CMCS. CMCS 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. Organizations may task the CMCS personnel with the responsibility for ensuring that the CMA has been verified by consulting the information contained in Safeguards and Security Information Management System (SSIMS). Additionally, it is the responsibility of the sender, not CMCS personnel, to provide the transmittal letter (when required) to be included in the package with the classified matter.

CMCS 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 CMCS 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 Confidential matter being hand carried inside the facility unless the receipt is used to document what matter is being hand carried or it is being transferred to another CMCS.

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

For all classified matter hand carried outside of a facility, a copy of the receipt, or other manifest, is left with the servicing CMCS, and one signed UNCLASSIFIED copy is carried on the person hand carrying the package. If the hand carried matter is returned to the same CMCS, 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 returns the receipt to the CMCS. 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 CMCS, or certify the destruction using a DOE F 5635.9, *Record of Destruction*. The DOE F 5635.9 should be given to the appropriate CMCS 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 CMCS on the same day is on record with the CMCS. All hand carried classified matter is reconciled upon return to the facility.

Classified Facsimiles:

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

If the classified facsimile machine is a stand-alone CMCS, Primary and, if applicable, Alternate Control Station Operators are appointed and listed in the Appendix to the local security plan in the same manner as a normal CMCS.

Although CMCS personnel may be 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 comply with all the established procedures. Transmission of classified information via facsimile machines that are not accredited for classified operation by the Office of the Chief Information Officer (OCIO) is strictly prohibited.

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 or access authorization, 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 are confirmed with the intended recipient. Facsimile logs, or separate receipts, are 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 is 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 are resolved immediately.

Appropriate classification markings, as in any classified document, are required for all incoming and outgoing classified facsimiles. Specific attention is 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 are applied to all incoming classified facsimiles immediately after receipt and before distribution.

Points of Contact:

For information on CMCS contact your ODFSA; or for policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Sample Notification for Authorized Recipients to Receive Classified Mail or Overnight Express Packages. (See Example 10-1.)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to: http://energy.gov/sites/prod/files/cioprod/documents/Form_470_10_fillable_X.pdf)

DOE F 5635.9, *Record of Destruction* (for a copy of this form go to http://energy.gov/sites/prod/files/cioprod/documents/5635-9.pdf)

Helpful Websites:

The HQ CMPC Program website is at: https://powerpedia.energy.gov/wiki/CMPC

To view the *DOE CMPC Marking Resource*, go to: http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

INTENTIONALLY LEFT BLANK

EXAMPLE 10-1

Sample Notification for Authorized Recipient to Receive Classified Mail or Overnight Express Packages

This information is sent from the ODFSA or their Authorized Recipient to the CMCS personnel as well as to the Mail Room personnel. It should include the following information:

The Subject should be titled, "Notification of Authorized Individuals to Receive Classified Mail or Overnight Express Packages" or similar language

The body should include the following information:

- The following personnel are authorized to receive and open classified (*insert USPS mail or overnight Express mail as appropriate*) addressed to (*enter appropriate information to identify the appropriate CMCS location*)

    - Name of Authorized Recipient:
    - Security Clearance Level or Access Authorization:
    - Organization code and/or organizational name:
    - Building name:
    - Room number/location of Classified Matter Control Station:
    - Telephone number:

- Repeat the above information, as necessary, to identify all Authorized Recipients. At the end of the notification add the signature of the authorized individual from the Mail Room, ODFSA or their Authorized Recipient as appropriate.

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

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

INTENTIONALLY LEFT BLANK

Section 11

Receipt and Transmission of Classified Matter

This section describes procedures for the receipt and transmission of classified matter. The federal facilities that are authorized to receive and transmit classified matter is identified in the local security plan. Department of Energy (DOE)-approved contractor sites are permitted to receive and transmit classified matter in accordance with their DOE contract(s), their Facility Data and Approval Record (FDAR) form (DOE F 470.2), and their security plan(s).

Implementation Guidance:

All classified matter received or transmitted to a site or facility is processed through a Classified Matter Control Station (CMCS) (see Section 10, Classified Matter Control Stations). CMCS personnel are responsible for receiving all classified matter addressed to the organizational element and transmitting all classified matter dispatched by the element. In short, the organizational element's CMCS is the organization's gateway for all incoming and outgoing classified matter. The CMCS should also maintain the associated classified document receipts and any required inventory records. If the associated classified document receipts and inventory records are kept elsewhere, it is indicated in the local security plan.

Receiving Classified Matter by Mail;

All mail, including express mail, is initially received by the site or facility Central Mail Room, as documented in the local security plan. 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 CMCS personnel who have been specifically designated to receive classified and express mail (see Section 12, Classified Mailing Addresses, and Section 13, Express Mail Service).

Receiving Classified Matter by Facsimile;

A classified facsimile machine is, in itself, a CMCS or part of an existing CMCS. Guidance for receiving classified facsimiles are contained in Section 10, Classified Matter Control Stations.

Classified Mailing Addresses;

All classified mail being sent to an organizational element, site or facility via the United States Postal Service (USPS) or other mail, express mail or delivery service uses the proper classified mailing address (CMA) as identified and confirmed in Safeguards and Security Information Management System (SSIMS).

The local security plan lists the appropriate CMA, the cognizant ODFSA, and a list or the location of a list of any additional Authorized Recipients along with the address.

For example, at DOE Headquarter (HQ), the security plan would provide:

- The classified mailing address for HQ organizational elements located at Forrestal and 955 L'Enfant Plaza facilities is:

  ATTN: (ORGANIZATION)
  US DEPT OF ENERGY
  PO BOX 23865
  WASHINGTON, DC 20026-3865

  List of Authorized Recipients: ODFSA and (other Authorized Recipients)

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

  ATTN: (ORGANIZATION)
  US DEPT OF ENERGY
  PO BOX A
  GERMANTOWN, MD 20875-0963

  List of Authorized Recipients: ODFSA and (other Authorized Recipients)

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 obtains written authorization from the ODFSA or their designee before transmitting classified matter outside of the facility.

The CMCS servicing the location is normally 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 ODFSA ensures training for CMCS personnel throughout the year.

The individual for whom the CMCS is transmitting the classified matter is responsible for knowing the name of the intended recipient, verifying that he/she has the appropriate security clearance or access authorization, and ensuring that he/she has a need-to-know. CMCS 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 CMCS procedures delegate that responsibility to some other individual(s).

Transmission of Top Secret Matter;

Top Secret matter may be transmitted out of a site or facility only by the Defense Courier Service, Department of State Courier System, approved communications networks (including approved classified facsimile), other ODFSA designated couriers or hand carry personnel (as designated by the organizational hand carry approval authority). Use of the USPS or other commercial organizations is prohibited.

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

A Local ODFSA Approved Courier Service – The approved Courier Service may be used to transmit Top Secret, Secret, and Confidential matter (*enter the local approved areas – for example, at DOE HQ it is defined as between the Forrestal and Germantown facilities or other Federal agencies within the Washington, D.C. metropolitan area*). Classified matter is **double wrapped**, properly marked, addressed to the proper CMA, and then placed in an approved red and white ("Candy Stripe") envelope or other additional 3rd outer wrapper approved by the ODFSA. A receipt is attached to that 3rd wrapping, and the transaction logged into the courier's register. All signatures on the receipt are accompanied by the signer's DOE badge number or printed name. Both the outer 3rd wrapping and the receipt 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 is also accompanied by DOE F 470.10, *Classified Document Receipt*, or equivalent. These receipts are retained for 5 years for Top Secret and 2 years for Secret and Confidential matter.

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

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

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

Express mail services is not 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 are met concerning express mail,

- Only designated CMCS personnel may prepare express mail packages for dispatch,

- Only commercial express mail service organizations authorized by contract with the General Services Administration (GSA) for outgoing classified express mail (overnight mail) may be used. (Note: On rare occasions, a recipient organization may only accept incoming express mail service from a carrier other than the one(s) approved by ODFSA for your site or facility. The recipient's requirement to use a different carrier is recorded in SSIMS. Other government agencies (OGAs) may send express mail to DOE via other carriers,

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

- For example, the return address on DOE Headquarter 's transmitted express mail is:

    - Forrestal: Sender's Name (Routing Symbol)

      US Department of Energy
      1000 Independence Ave SW
      Washington, DC 20585

    - Germantown: Sender's Name (Routing Symbol)

      US Department of Energy
      19901 Germantown Rd
      Germantown, MD 20874

Transmissions by Secure Telephone Equipment (STE):

A STE device is used to transmit classified information telephonically. STEs are used within an approved security area (e.g., limited area (LA) or vault type room (VTR)) unless specifically approved. The voice and storage requirements are approved by the ODFSA. For sites with multiple ODFSAs, an ODFSA may re-delegate responsibilities to a local Technical Surveillance Countermeasures Operations Manager provided all site ODFSAs agree to the re-delegation. Key and other controlled cryptographic items required off-site is approved by the Director, Technical Security Program, who also serves as the Central Office of Record (COR). Additional information on secure communications can be found in DOE Order 470.6, *Technical Security Program*.

Participants in classified STE communications ensure that conversations cannot be overheard by individuals without proper access authorization and need-to-know.

Packaging Classified Matter for Transmission Outside of a Facility:

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

- Envelopes – When envelopes are used for packaging, the classified matter is 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 is sealed and marked with the receiver's and the sender's classified mailing addresses, the overall classification level and category (if Restricted Data (RD), Formerly Restricted Data (FRD), or Transclassified Foreign National Information (TFNI)) of the contents, and any appropriate caveats. The outer envelope is sealed and marked with the receiver's and the sender's classified mailing addresses. No markings or notations are made on the outer envelope indicating that the contents are classified. All seams of both wrappings are sealed with brown sealing paper tape to aid in preventing undetected, unauthorized access to the contents while in transit.

- 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 are used to protect the item while in transit. Both the inner and outer containers are marked as stated in the above paragraph.

- Locked Briefcases – A locked briefcase may be authorized by the ODFSA for hand carrying of classified matter within a facility. If a locked briefcase is used to hand carry classified matter of any level outside a facility within a locally designated vicinity, the briefcase may serve as the outer container (wrapper). The inner container is 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) indicates the classified mailing address of the carrier and contains 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 an OGA when the intention is to leave the classified matter at the destination.

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

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

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

  - Standard classification and addressing markings are 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 or 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.

- 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 are used for classified matter transmitted outside a 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 Facilities (Other Than Hand Carrying);

Non-hand carried classified matter transmitted between facilities is handled by the organizational element's CMCS. The CMCS uses their internal established procedures to coordinate with the mail room or Courier Service to effect the transmittal.

Classified Document Receipts;

An appropriately prepared DOE F 470.10, *Classified Matter Receipt*, accompanies all accountable and Secret documents transmitted outside a facility and are enclosed within the inner envelope or container. A receipt is also used when classified information is transferred to a foreign government or its representative. 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 is 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 is maintained for *all* classified matter, regardless of classification level, that is hand carried or couriered outside of a facility.

Hand Carrying of Classified Matter within a Facility; Classified matter that will be hand carried to personnel located in a separate LA or VTR within a facility may be carried by personnel having an appropriate access authorization for the level and category of classified matter involved as authorized by the local security plan. The matter has 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 is transported within a red and white striped envelope and marked with the recipient's name, room number, routing symbol, and telephone number. The matter is not visible through the red and white striped envelope. A receipt may also be used when the matter will not be returned to the CMCS or for documentation of the movement, such as in the case of accountable matter.

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 a facility 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 ODFSA for each facility designates in writing a responsible official (e.g., ODSA) within the organizational element to approve employees to hand carry classified matter out of a facility. This authority should be limited to as few individuals as operationally feasible.

The individual(s) designated by the ODFSA to approve employees within the organization to hand carry classified matter maintains a record of those granted the authority to hand carry. Employees are approved each time classified matter is hand carried outside the facility.

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

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

Travelers do 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 are 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, is stored only in DOE-approved facilities, or as specified in approved contingency plans. Arrangements are made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

The individual(s) designated by the ODFSA to approve employees within the organization to hand carry classified matter ensures 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 Example 11-1. A record of hand carry briefings is maintained. Each briefing includes, 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 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 ODFSA to approve employees within the organization to hand carry classified matter provides approval each time classified matter is to be hand carried outside the facility. Repeated approval for hand carrying classified matter within the facility is not required and is valid until rescinded by the appropriate authority. Hand carrying classified matter outside the facility 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 organizational element. A *Sample Hand Carry Contingency Plan* is provided in Example 11-2,
- Point(s) of contact for assistance.

A record is made for *all* classified matter, regardless of classification level, that is hand carried outside a facility. An **Unclassified** copy of this record will be in the possession of the employee who hand carries the classified matter, and a copy of the record is also maintained by the organizational element's CMCS. 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 other record includes --

- Unclassified 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, CMCS personnel 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 ODFSA or his/her designee. The purpose of the airport guidance 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.

INTENTIONALLY LEFT BLANK

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 presents 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:*
    a. *Full name of the agency*
    b. *Full name of the courier*
    c. *Date of issue and expiration date of the assignment*
    d. *Full name, signature, and telephone number of the official issuing the letter, card, or form*
    e. *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 is from the Head of the HQ Departmental Element/Program Office, through the Field Office, ODFSA or his/her designee and is 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 Example 11-3.

The classified package is 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 except as noted below. However, in rare circumstances, the Head of the HQ Departmental Element/Program Office, Field Office, or the ODFSA may approve the transmission on a case-by-case basis as authorized.

> *NOTE: Approval from the U.S. Department of State Bureau of Diplomatic Security (DS), Office of Diplomatic Courier Services (DS/C/DC) is 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 is to be carried or the post to which the pouch is addressed within the time that official business will be conducted.**

Nonprofessional couriers are U.S. citizens and full-time direct hire U.S. government employees; have a Top Secret security clearance (or DOE "Q" access authorization if carrying RD classified matter), a diplomatic passport, a diplomatic visa, 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 is enclosed in sealed diplomatic pouches obtained from DS/C/DC until delivered to its official destination.

Several other conditions are required before DOS will authorize a nonprofessional courier to hand carry classified matter across international borders. Contact the ODFSA for additional information.

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 your cognizant Program Office/HQ Departmental, Field Office or ODFSA 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 (301) 903-2644.

For information on local transmission and receipt information contact your ODFSA or for policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Sample Briefing for Persons Authorized to Hand Carry Classified Documents (see Example 11-1)

Sample Hand Carry Contingency Plan (see Example 11-2)

Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material (see Example 11-3)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to: http://energy.gov/sites/prod/files/cioprod/documents/Form_470_10_fillable_X.pdf)

Other Reference:

DOE Order 142.2A, Admin Chg 1, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency.*

Helpful Websites:

The HQ CMPC Program website is at: https://powerpedia.energy.gov/wiki/CMPC.

To view the *DOE CMPC Marking Resource*, go to: http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource

INTENTIONALLY LEFT BLANK

EXAMPLE 11-1

SAMPLE BRIEFING FOR PERSONS AUTHORIZED TO HAND CARRY CLASSIFIED DOCUMENTS

Hand Carrying of Classified Matter Briefing:

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 Matter Control Station (CMCS) 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 is coordinated through your servicing CMCS. 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 return to your CMCS 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 facility, your security clearance or access authorizations, SCI accesses, Sigma or other special accesses should be passed to the receiving 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 within a site or facility, your standard DOE security badge may be accepted as proof that you are authorized to hand carry classified matter (check the requirements in your local security plan). You should inform your CMCS of your intention to hand carry classified matter and process it through your CMCS to assist in the preparation of the documents, package, and required labels. As stated above, you return to your CMCS 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 facility, specific authorization from your OSFSA 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:

- Individuals hand carrying classified matter possess an access authorization commensurate with the level of information being hand carried and be aware of their responsibility to continuously safeguard classified information.

- You will 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 is appropriately marked and wrapped.

If you lose or misplace any classified matter, or if it is compromised or possibly compromised, you will report the situation immediately to your ODFSA or their designee. If the incident occurs during non-working hours, you will 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
_____	_____	_____

EXAMPLE 11-2

Sample Hand Carry Contingency Plan

Anyone hand carrying classified matter is 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 *(insert appropriate office information)*. 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.

A contingency plan is explained and a copy provided to the cognizant Classified Matter Control Station (CMCS) each time classified matter is hand carried.

The following plans are provided as examples of a hand carry contingency plan used at DOE HQ (please note that at HQ **the HSO as listed below in the example may be equivalent to the ODSA at other sites and facilities**):

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

1. The DOE security badge at the appropriate level and category 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 is double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the individual's CMCS.

3. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* is included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office's CMCS. 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 will contact his/her HQ Security Officer (HSO) and inform him/her of the situation. The Office of (*appropriate office information)* HSO may be reached at (*telephone number)* during regular hours. After regular hours, or if the HSO is unavailable, the Emergency Operations Center can be contacted 24 hours per day at (*telephone number).*

5. If the classified matter cannot be delivered promptly to the intended recipient, it will 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 will be notified *immediately*.

Sample HQ 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, other government agencies (OGA), or the U.S. Congress, has his/her security clearance or access authorization, 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 ensures 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 *(insert appropriate office information)* Classified Matter Control Station (CMCS) Operators.

3. All classified matter is double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the Office of *(insert appropriate office information)* CMCS.

4. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* is included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office of *(appropriate office information)* CMCS. 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 will contact his/her HSO and inform him/her of the situation. The HSO may be reached at *(insert telephone number)* 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 (*insert telephone number)*. These numbers are also printed on the hand carry authorization card.

6. If the classified matter cannot be delivered promptly to the intended recipient, it will 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 local DOE site approved for storing classified matter at the level and category being hand carried.

- A local DOE contractor facility approved for storing classified matter at the level and category being hand carried.

- A local U.S. military installation with the capability to store classified matter at the level and category being hand carried.

- A local FBI office with the capability to store classified matter at the level and category being hand carried.

- 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

If the classified matter is turned over to one of the above entities, the package will 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 will be reported immediately to the HSO.

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

9. 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 applies in protecting the classified matter. In any situation or circumstance, you will 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.

INTENTIONALLY LEFT BLANK

EXAMPLE 11-3

Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material (on 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 (insert appropriate office information), 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: U.S. 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

INTENTIONALLY LEFT BLANK

Section 12
Classified Mailing Addresses

Classified matter is addressed only to approved Classified Mailing Addresses (CMAs) contingent upon the appropriate method of transmission (i.e., mailing, shipping, or overnight express delivery). The Classified Matter Control Station (CMCS) operator will consult Safeguards and Security Information Management System (SSIMS) to verify the CMA and the authorized storage capability of the receiver before dispatching the matter. In some cases the Department of Defense Security Services (DSS) can provide classified mailing addresses.

This section describes the procedures for obtaining various CMAs.

Implementation Guidance:

It is recommended that there is least one person assigned to the CMCS or at least each facility who is 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 at your site or facility has access to SSIMS, contact the ODFSA.

> *NOTE 1: SSIMS is an automated classified database that is accessed through an information system approved and accredited to process classified information. Individuals requiring access to SSIMS should initially contact their Information Security Oversight Office (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.*

<u>CMAs for DOE HQ Organizational Elements</u>;

CMAs for DOE HQ organizational elements are available in SSIMS. Each is registered in SSIMS as either a non-possessing or possessing facility. The FDAR for each HQ Organizational Element reflects whether it 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 organizational element's storage capability.

<u>CMAs for Other DOE Federal Facilities</u>;

CMAs for all non-HQ DOE facilities are also 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 (OGAs),

CMAs for OGAs are 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 are 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:

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

To contact the Office of Information Security (AU-42), call (301) 903-9990.

For local information on CMAs, contact your ODFSA; or for policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

DOE F 470.2, *Facility Data and Approval Record,* (for a copy of this form go to: http://energy.gov/sites/prod/files/cioprod/documents/470-2%281%29.pdf).

Helpful Website:

The HQ CMPC Program website is at: https://powerpedia.energy.gov/wiki/CMPC.

Section 13

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, Classified Matter Control Station (CMCS) personnel release all express mail packages directly to the person to whom it is addressed (addressee) or other individual identified in the local security plan for the safe-keeping of the document for the intended recipient. If the addressee is not available, the express mail package may be released to another person who has been specifically appointed by the ODFSA) or their designee to receive and open such packages.

NOTE: Top Secret (TS) matter may not be transmitted via express mail.

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

Implementation Guidance:

Appointment of Personnel to pick up Express Mail Documents or Packages.

Each ODFSA or their designee designate personnel before they can pick up express mail packages from the Mail Room Express Mail Office on behalf of personnel within their organizations.

The organizational element's ODFSA or their designee submits a list of the organization's authorized personnel to their Mail Room Express Mail Office. ODFSAs or their designees use the *Sample Email Notification for Express Mail Document Control Authorized Recipients* (Example 13-1) or equivalent to inform the Mail Room of these individuals. When there are changes to the Authorized Recipients, the ODFSA or their designee immediately notify the Mail Room of the changes.

NOTE: The Mail Room Express Mail Offices are not authorized to release an express mail package to anyone other than the addressee or an individual on this list of personnel authorized to pick up express mail packages.

Each location is as either a possessor or non-possessor of classified matter:

1. Possessing Organizational Elements are those facilities that can receive and store classified matter. Individuals designated to pick up express mail at these facilities have a "Q" or "L" access authorization or a "TS," "S", or "C" security clearance at the same level or higher classification of the highest potential level of the matter. CMCS personnel (see Section 10, Classified Matter Control Stations) may also serve in this capacity.

2. Non-Possessing Organizational Elements are those facilities that are not approved to receive or store classified matter at any of their facilities. Those individuals designated to pick up mail for a Non-Possessing Organizational Element are not required to possess either a "Q" or "L" access authorization or a TS, S, or C security clearance.

Incoming Express Mail Packages to a Possessing Facility or Organizational Element**;**

On the day the express mail package is received, the Mail Room Express Mail Office notifies the addressee.

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

Unless specifically prohibited, only the addressee or the cleared individual(s) who are authorized to retrieve packages from the Express Mail Office may do so. 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 is taken immediately to their CMCS for proper processing and/or storage. In any event, express packages are not 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 individual authorized to pick up classified matter for the addressee is unavailable or does not pick up the package by early afternoon of the following day, the Express Mail Office contacts the ODFSA or their designee for the recipient's organization and requests that arrangements be made for the package to be retrieved by a cleared employee or the addressee. On the morning of the third day, if the package has not been picked up by then, the Express Mail Office notifies the ODFSA again to decide what action to take on the undelivered package. If no decision can be made, the Head of the Organizational Element is contacted.

If the package was picked up by and opened by CMCS personnel within a security area, the identity of the addressee is determined as to whether or not they have the appropriate clearance or access authorizations for the classified matter. If they do, the document is processed accordingly through their CMCS. If they don't or if the package was picked up and opened by the addressee in a non-security area and they did not have the appropriate clearance or access authorizations for the classified matter, the ODFSA should be notified of a potential incident of security concern (IOSC).

Outgoing Express Mail Packages from a Possessing Facility or Organizational Element;

If an outgoing express package contains classified matter, it is handled by the organizational element or facility's CMCS 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 a Non-Possessing Facility or Organizational Element;

On the day the express mail package is received, the servicing Express Mail Office notifies the addressee. The addressee or individual authorized to pick up express mail 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 the addressee opens the package and finds classified, they immediately notify the ODFSA of an IOSC.

If the package has not been picked up from the Mail Room by early afternoon of the following day, the Express Mail Office contacts the designated ODFSA for the recipient's organization. On the morning of the third day, if the package has not been picked up, the Express Mail Office again notifies the ODFSA to determine what action to take regarding the package. If no decision can be made, the Head of the Organizational Element is contacted.

Outgoing Express Mail from a Non-Possessing Facility or Organizational Element;

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

In the uncommon event that a non-possessing organizational element transmits classified matter via express mail, an appropriately cleared person (e.g., the ODFSA) coordinates with the CMCS of a possessing organizational element to effect this transmission.

Express Mail Pick Up Authorized Recipient or Addressee Responsibilities;

Express mail pick up Authorized Recipient or addressees immediately pick up express mail packages when contacted by the Mail Room Express Mail Office. Upon return to their respective office or designated security area, they 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 wrapping or the contents, 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 express mail pick up Authorized Recipient does not meet these requirements, they do not open the package any further and immediately contact the organization's ODFSA or CMCS personnel for additional guidance.

NOTE: If the individual cannot locate CMCS personnel, the ODFSA, a cleared ODSA or ODSA Representative, he/she immediately contacts the Head of the Organizational Element for assistance.

Point of Contact:

For information about the local CMPC Program requirements, contact your ODFSA; or for policy information E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Sample E-mail Notification for Express Mail Document Control Authorized Recipients (see Example 13-1).

Helpful Website:

The HQ CMPC Program website is at: https://powerpedia.energy.gov/wiki/CMPC.

EXAMPLE 13-1

Sample Notification for Express Mail Document Control Authorized Recipients

Send the notification to: "Mail Room Express Mail Office"

"Subject" block should be: "Notification of Authorized Individuals to Accept Express Mail" or similar language

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

The Office of *(insert appropriate office information)* has approved the following personnel to receive and open express mail packages addressed to this office:

Name of Individual,
Security Clearance or Access Authorization Level,
Organization code and/or organizational name,
Building name,
Room number/location of Classified Matter 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 Authorized Recipients, 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 listing that the person is no longer approved to receive and open classified mail and include the word "DELETE" behind the person's name.

Notifications should be accepted only from the organizational element ODFSA or their designee.

INTENTIONALLY LEFT BLANK

Section 14

Destruction of Classified Matter

This section describes how to properly destroy classified matter.

Implementation Guidance:

Organizational 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 are 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 is requested from the DOE Office of General Counsel.

Approved Methods of Destruction:

Classified matter is destroyed beyond recognition to preclude reconstruction. Equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. However equipment approved for use prior to January 1, 2011, and not found on an EPL, may be utilized for the destruction of classified information until December 31, 2016.

The approved methods of destruction are;

Shredders – Crosscut shredders are approved for the destruction of all classified **paper documents**. The shredder reduces 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, ODFSAs or their designee should check the particulate output of the shredders used by their organizational 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 are taken out of service.

Crosscut shredders that produce a particulate size that meets the above requirement may be approved by the ODFSA. Shredders approved by ODFSAs for classified destruction

are located in limited areas (LAs) or vault type rooms (VTRs) and are designated by conspicuously posted signs. Shredders **approved** for classified destruction have the sign posted either on the equipment or nearby. The sign contains the make and model of the shredder and is signed and dated by the appropriate ODFSA or their designee. A sample of the sign is provided in Example 14-1. All shredders located in an LA or VTR that are **not approved** for destruction of classified matter have a *Not Authorized for Classified Destruction* sign posted on the shredder (provided in Example 14-2).

Centralized Classified Destruction Facility (CCDF) – A CCDF may be established and 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). The CCDF is approved by the ODFSA prior to operation to ensure that it meets all destruction requirements for each type of matter destroyed in it.

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 ODFSA, 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 has a security clearance or access authorization 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 their offices are 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) are sorted into separate, properly annotated classified burn bags not to exceed the designated number of pounds in weight as documented in the destruction procedures in the local security plan. 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 are removed from all paper documents and waste. Bags containing fasteners of any kind may be returned to the originator.

- Classified burn bags 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, is clearly marked on the side of each bag for identification. The weight of the matter within each burn bag is limited as documented in the destruction procedures in the local security plan. 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 collection points listed in the destruction procedures portion of the local security plan during the times stipulated.

Destruction of Accountable Classified Matter;

The destruction of accountable classified matter is witnessed by an appropriately cleared individual other than the person destroying the matter. Both the destruction official and the witness have a security clearance or access authorization 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 security clearance or access authorization contact the ODFSA or their designee for guidance on destruction.

A DOE F 5635.9, *Record of Destruction*, or equivalent, is completed whenever accountable classified matter is destroyed. An operator within the organizational element's CMCS authorizes the destruction and maintains all DOE F 5635.9s or other destruction records and 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 ODFSA-approved crosscut shredder or at the CCDF. When using the CCDF, paper, plastics and metal is 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, is 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.

When a CCDF is available, a destruction appointment is made by calling the CCDF operator at the phone number included in the destruction procedures portion of the local security plan. 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 organizational element destroying the accountable matter provides 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 9, Classified Matter Accountability, for examples of accountable classified matter.

Points of Contact:

For information on the local destruction procedures, contact your ODFSA or their designee.

For information on destruction policy, E-mail: Security.Directives@hq.doe.gov.

Forms/Samples/Graphics:

Sample Authorized for Classified Destruction Sign (see Example 14-1).

Sample Not Authorized for Classified Destruction Sign (see Example 14-2).

DOE Form 5635.9, *Record of Destruction* (for a copy of this form go to: http://energy.gov/sites/prod/files/cioprod/documents/5635-9.pdf).

Helpful Website:

For U.S. Government Standard Forms go to: http://www.gsa.gov/portal/forms/type/SF

For media destruction guidance go to:
https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/

EXAMPLE 14-1

Sample Authorized for Classified Destruction Sign

EXAMPLE 14-2

Sample Not Authorized for Classified Destruction Sign

Section 15

Incidents of Security Concern

This section describes Incidents of Security Concern (IOSC) involving classified information.

Implementation Guidance

IOSCs include a range of possible actions, inactions, or events that:

- Pose threats to national security interests and/or Departmental assets;
- Create potentially serious or dangerous security situations;
- Have a significant effect on the Safeguards and Security (S&S) Program's capability to protect DOE S&S interests;
- Indicate the failure to adhere to security procedures; or
- Illustrate the system is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

Whenever there is an observation, finding, or knowledge of information which may indicate an IOSC, it is immediately reported to the ODFSA or designee as documented in the local security plan using the most secure means available. Reasonable and prudent steps are taken to contain the incident, protect the scene and secure classified matter, as appropriate. The specific requirements for the categorization, initial report, inquiry process and closure reports may be found in DOE Order 470.4B, *Safeguards and Security Program*.

Points of Contact:

For information on the local IOSC procedures, contact your ODFSA or their designee.

For information on IOSC policy, E-mail: Security.Directives@hq.doe.gov.

INTENTIONALLY LEFT BLANK

References

The following provides a list of the Departmental and national policy documents adopted by Department of Energy (DOE) as they relate to Classified Matter Protection and Control (CMPC):

Title 10 Code of Federal Regulations (CFR) 1045
Description Nuclear Classification and Declassification
URL https://pir.doe.gov/collection
Abstract:
This part establishes a program for managing, identifying, generating, reviewing, and declassifying restricted data and formerly restricted data; it also establishes the sanctions for violations of the procedures.

Title 10 CFR 824
Description Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations
URL https://pir.doe.gov/collection
Abstract:
This part establishes penalties for any person who has entered into a contract or agreement with the Department of Energy and who violates (or whose employee violates) any applicable rule, regulation, or order under the Atomic Energy Act relating to the security or safeguarding of restricted data or other classified information.

Title 32 CFR 2001
Description Classified National Security Information
URL http://www.GPO.gov

Abstract:
This part prescribes a uniform system for classifying, safeguarding, and declassifying national security information; it also establishes a monitoring system to enhance its effectiveness.

Title DoD 5220.22-M, Chg 2
Description National Industrial Security Program Operating Manual, 18 May 2016, Change 2
URL http://www.dss.mil
Abstract:
This establishes enhanced security requirements for special access programs and sensitive compartmented information. A summary of changes can be found at: http://www.dss.mil

Title DoD 5220.22-R
Description Industrial Security Regulation
URL https://pir.doe.gov/collection

Abstract:
This document establishes policies, practices, and procedures of the Department of Defense Industrial Security Program used internally by the Department of Defense to ensure maximum uniformity and effectiveness in its application throughout industry.

Title Classification Bulletin GEN-16 Revision 2
Description "No Comment" Policy on Classified Information in the Open Literature
URL http://energy.gov/ehss/downloads
Abstract:
Provides guidance to DOE Federal and contractor employees with access to classified information on appropriate actions when classified information (i.e., Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), and National Security Information (NSI)) appears in the open literature and to clarify the circumstances that constitute comment.

Title DOE O 241.1B
Description Scientific and Technical Information Management
URL https://www.directives.doe.gov/directives-documents/200-series/0241.1-BOrder-b
Abstract:
This order establishes requirements and responsibilities to ensure access to classified and unclassified controlled scientific and technical information is controlled in accordance with legal or Department of Energy requirements.

Title DOE O 251.1C
Description Departmental Directives Program
URL https://www.directives.doe.gov/directives-documents/200-series/0251.001-BOrder-c
Abstract:
This order defines requirements and responsibilities for implementing the Department of Energy (DOE) Directives Program in support of the Secretary's memorandum of September 10, 2007, Principles Governing Departmental Directives.

Title DOE O 452.6A
Description Nuclear Weapon Surety Interface with the Department of Defense
URL https://www.directives.doe.gov/directives-documents/400-series/0452.6-BOrder-a
Abstract:
This order establishes Department of Energy and National Nuclear Security Administration requirements and responsibilities for addressing joint nuclear weapon and nuclear weapon system surety activities in conjunction with the Department of Defense.

Title DOE O 452.7
Description Protection of Use Control Vulnerabilities and Designs
URL https://www.directives.doe.gov/directives-documents/400-series/0452.7-BOrder

Abstract:
This order establishes the policy, process, and procedures for control of sensitive use control information in nuclear weapon data categories Sigma 14 and Sigma 15 to ensure that dissemination of the information is restricted to individuals with a valid need to know.

Title DOE O 452.8
Description Control of Nuclear Weapon Data
URL https://www.directives.doe.gov/directives-documents/400-series/0452.8-BOrder
Abstract:
The directive establishes the policy, process and procedures for control of nuclear weapon data to ensure that dissemination of the information is restricted to individuals with appropriate clearances, approved authorization and valid need-to-know in keeping with the Atomic Energy Act (as amended) stipulation of ensuring common defense and security.

Title DOE O 470.4B, Admin Chg 1
Description Safeguards and Security Program
URL https://www.directives.doe.gov/directives-documents/400-series/0470.4-BOrder-b-admchg1
Abstract:
This Order establishes responsibilities for the U.S. Department of Energy (DOE) Safeguards and Security (S&S) Program, and establishes program planning and management requirements for the S&S Program.

Title DOE O 470.6
Description Technical Security Program
URL https://www.directives.doe.gov/directives-documents/400-series/0470.6-BOrder
Abstract:
This order implements the Department of Energy (DOE) Technical Security Program (TSP). This program represents the convergence of two distinct disciplines: Counterintelligence (CI) and Security Countermeasures. The elements of the TSP are driven by national level, interagency programs that are codified in various laws, Executive Orders, national polices and directives.

Title DOE O 471.5
Description Special Access Programs
URL https://www.directives.doe.gov/directives-documents/400-series/0471.5-BOrder
Abstract:
This order is Official Use Only and will not be distributed on the directives portal. For distribution, please contact the Executive Secretary of the Special Access Program Oversight Committee at 202-586-6775.

Title DOE O 471.6, Admin Chg 2
Description Information Security

URL https://www.directives.doe.gov/directives-documents/400-series/0471.6-BOrder-admchg2

Abstract:
This Order establishes requirements and responsibilities for Department of Energy (DOE) Departmental Elements, including the National Nuclear Security Administration (NNSA), to protect and control classified information as required by statutes, regulation, Executive Orders, government-wide policy directives and guidelines, and DOE policy and directives

Title DOE O 472.2 Chg 1
Description Personnel Security
URL https://www.directives.doe.gov/directives-documents/400-series/0472.2-BOrder-chg1-pgchg

Abstract:
The order establishes requirements that will enable DOE to operate a successful, efficient, cost-effective personnel security program that will ensure accurate, timely and equitable determinations of individuals' eligibility for access to classified information and Special Nuclear Material. This limited revision will ensure that individuals holding dual citizenship receive proper consideration from a counterintelligence perspective prior to being granted access to classified matter or Special Nuclear Material.

Title DOE O 475.2B
Description Identifying Classified Information
URL https://www.directives.doe.gov/directives-documents/400-series/0475.2-BOrder-b

Abstract:
This order establishes a program to identify and protect Restricted Data, Formerly Restricted Data, and Transclassified Foreign Nuclear Information.

Title ICD 700
Description Protection of National Intelligence
URL http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives

Abstract:
This Directive establishes Intelligence Community (IC) policy for the protection of national intelligence and intelligence sources, methods, and activities, greater coordination and communication between CI and security activities if the IC, and oversight of CI and security activities across the IC.

Title EO 12968
Description Access to Classified Information
URL https://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf

Abstract:
This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

Title EO 13526
Description Classified National Security Information
URL https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf
Abstract:
This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

Title SF 700 Security Container Form - Continuation Page
Description Security Container (SF-700) - Continuation Page
URL http://www.gsa.gov/portal/forms/download/115574
Abstract:
The continuation page is used to identify individuals with knowledge of the combination who are not listed on the SF-700 Part 1 & 2.

Title SF 700 Security Container Information Standard Form
Description SF-700 Security Container Information Standard Form
URL http://www.gsa.gov/portal/forms/download/115574
Abstract:
This form contains information--including location, container number, lock serial number, and contact information for the responsible party--about the security container in which the form is located.

Title SF 701 Activity Security Checklist
Description SF-701 Activity Security Checklist
URL http://www.gsa.gov/portal/forms/download/115578
Abstract:
This form is used for end-of-day security inspections and daily security checks on work areas.

Title CNSS Directive No. 502
Description National Directive on Security of National Security Systems
URL https://www.cnss.gov/CNSS/issuances/Directives.cfm
Abstract:
This directive clarifies objectives, policies, procedures, standards, and terminology set forth in NSD-42, National Policy for the Security of National Security Telecommunications and Information Systems.

Title CNSSP Directive No. 26
Description National Policy on Reducing the Risk of Removable Media
URL https://www.cnss.gov/cnss/issuances/Policies.cfm
This document is designated FOUO. To access protected FOUO content in the CNSS Library, you must login with a Federal/DoD Public Key

Infrastructure (PKI), Personal Identity verification (PIV) or Common Access Card (CAC) client certificate correctly installed in your browser.

Abstract:
This policy establishes the criteria for using removable media with national security systems.

Title ISOO 2011-02
Description Further Guidance and Clarification on Commingling Atomic Energy Information and Classified National Security Information
URL http://www.archives.gov/isoo/notices/
Abstract:
This Notice provides further guidance on marking commingled Transclassified Foreign Nuclear Information (TFNI) and classified National Security Information (NSI), and provides clarification on the placement of declassification instructions on single page documents that commingle Restricted Data (RD), Formerly Restricted Data (FRD), or TFNI, and classified NSI.

Title NSD 42
Description National Policy for the Security of National Security Telecommunications and Information Systems
URL https://www.hq.nasa.gov/office/pao/History/nsdd-42.html
Abstract:
This directive establishes a mechanism for policy development and dissemination; assigns responsibilities for implementation; and establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems (telecommunication and information processing systems) from exploitation.

Title NSDD 84
Description Safeguarding National Security Information
URL https://www.hsdl.org/?view&did=463004
Abstract:
This directive sets the requirements for protecting national security information against unlawful disclosures and requires individuals to sign a nondisclosure agreement before being granted access to sensitive compartmented information; the directive also establishes the requirements for procedures governing reporting and responding to unauthorized disclosures and authorizes agencies to adopt policies that require employees to submit to polygraphs in the course of unauthorized disclosure investigations.

Title 42 USC 2011
Description Congressional Declaration of Policy - Atomic Energy Act of 1954
URL http://www.gpo.gov/
Abstract:
This section governs the development, use, and control of atomic energy.

Title 42 USC 2164
Description International cooperation
URL http://www.gpo.gov/
Abstract:
This section provides for cooperation regarding data exchange that involves sensitive nuclear information between the United States and foreign nations.

Title 42 USC 2165
Description Security restrictions
URL http://www.gpo.gov/
Abstract:
This section requires contractors and prospective contractors to agree in writing that Restricted Data will not be disseminated to uncleared personnel, and it authorizes the Department of Energy to release Restricted Data during war or national disasters to persons awaiting access authorizations.

Title 42 USC 2274
Description Communication of Restricted Data
URL http://www.gpo.gov/
Abstract:
This section provides penalties for unauthorized communication of Restricted Data with intent to injure the United States or aid a foreign country.

Title 42 USC 2277
Description Disclosure of Restricted Data
URL http://www.gpo.gov
Abstract:
This section establishes criminal penalties for disclosing Restricted Data by a Federal or contractor employee to any person who he/she knows or has reason to believe is not authorized to receive it.

Title 42 USC 2282
Description Civil Penalties
URL http://www.gpo.gov
Abstract:
This section provides civil penalties for violations of licensing requirements, safety regulations, and security regulations related to classified and unclassified controlled information.

Title DOE CMPC Marking Resource, updated January 2015
Description Marking Documents
URL http://energy.gov/ehss/downloads/security-policy-cmpc-marking-resource
Abstract:
This resource provides examples of marked classified documents to include NSI e-mails.

Title DOE Office of Environment, Health, Safety and Security (EHSS) Safeguards and Security Policy Information Resource (S&S PIR).
Description Policy References
URL https://PIR.doe.gov
Abstract:
This is an excellent resource that links to national policy documents, DOE directives and requirements, national policy implementation, and resources such as glossary and acronyms, recent changes and crosswalk that provides a means to track the notification, addition, or deletion of safeguards and security directive requirements

Title Information Security Oversight Office (ISOO) Marking Classified National Security Information booklet. Revised January 2010
Description Marking Documents
URL http://www.archives.gov/isoo/training/marking-booklet.pdf
Abstract:
This booklet provides examples for marking classified NSI documents.

DEFINITIONS

Access: Ability to gain entry, retrieve, open, read, edit, view, carry or handle classified information.

Access Authorization: An administrative determination that an individual is eligible for access to particular types or categories of classified information or material (Indicates eligibility for Restricted Data at the appropriate classification level.)

Classified Matter Control Station (CMCS): Central location to manage the receipt or transmission of classified matter. A gateway for a particular location (organization, office, department, etc.) through which all incoming and outgoing classified matter transits, with the possible exception of e-mails which may or may not be required to be documented through the CMCS based on local procedures. This may include record keeping (accountable matter, training records, etc.) as defined by local security plan.

Classified Matter Control Station Operator: An individual with responsibilities within a Classified Matter Control Station.

Classified Signature Block: A term used in 32 CFR 2001 which is the same as the term "Classification Authority Block" used by DOE to provide information on the classifier, source and any declassification instructions required.

Classification Authority Block: Information on the classifier, source and any declassification instructions required. 32 CFR 2001 uses the term "Classified Signature Block" for the same thing.

Classification Category: The four classification categories used by DOE and Government are: Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI) and National Security Information (NSI).

Classification Level: The three classification levels are Top Secret (TS), Secret (S) and Confidential (C).

Classified Document Courier: An individual authorized to transport classified documents.

Classified Mailing Address: The address authorized to receive classified information as documented in the Safeguards and Security Information Management System (SSIMS) or Defense Security Service (DSS).

Custodian: An individual with storage responsibilities for classified matter. This includes classified maintained in safes, vaults, VTRs and other approved storage locations.

Defense Security Services (DSS): A Department of Defense organization who provides security services for various other agencies and organizations.

Departmental Element: Federal DOE Program Offices, Staff Offices and DOE Administrations, which have Federal oversight responsibilities for Laboratories, Technology Centers, Site Offices and Power Administrations.

Derivative Classifier: An individual appointed and trained to determine whether a document or material contains classified information or whether a document or material should be upgraded and responds to classification challenges received and forwards unresolved challenges to the Director, Office of Classification.

Deviation: Any departure or change from a requirement. Deviation or waiver is often used by other Government agencies. DOE uses the terms exemption or equivalency.

Equivalencies: Alternatives to how a requirement in a directive is fulfilled in cases where the "how" is specified. These represent an acceptable alternative approach to achieving the goal of the directive.

Exemption: A release from one or more requirements in a directive.

Foreign: A foreign government, a foreign national or individual, or a representative of a foreign government or entity.

Initial Security Briefing: Briefing provided to individuals at the time they receive their security badge.

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Insider Threat: The threat posed that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Need-to-know (NTK): Access to classified information required by an individual with the appropriate security clearance or access in the performance of official duties. The responsibility for determining need-to-know in connection with classified information rests with the individual who will disclose classified information. Need-to-know is based on an assessment that the receiving individual has a bona fide need to access the information in furtherance of an official Governmental purpose.

Officially Designated Federal Security Authority (ODFSA): A Federal employee with delegated authority and responsibilities for assigned CMPC duties as directed by the head of the Program Office/HQ Departmental Element through the Cognizant Security Office (CSO). They are designated as the primary point of contact for all CMPC activities within the HQ Departmental Element/Program Office's organizational element by a documented delegation. The ODFSA is responsible for ensuring CMPC procedures to implement the requirements of

applicable laws, Executive Orders, and DOE directives are developed for each site or facility under their responsibility and within their delegated authority. The ODFSA may further delegate other personnel to fulfill specific duties assigned to them through a delegation of authority. While an ODSA may be a Federal or contractor employee, contractors may not be delegated inherently Federal duties. The ODFSA remains responsible for all tasks originally delegated to them, including those delegated to others.

Office of Primary Interest: The DOE Office or National Nuclear Security Administration that is responsible for the development of a specific DOE directive (Order, Notice, Guide, and/or Technical Standard). The OPI is consulted on requests for exemptions and equivalencies on existing directives when required.

Officially Designated Security Authority: An individual with documented, delegated authority and responsibilities as directed through the head of the HQ Departmental Element/Program Office, Field Office and ODFSA as applicable. They are designated certain responsibilities as documented in their delegation. They may be a Federal or contractor employee; however, a contractor cannot be delegated Federal responsibilities.

Organizational Element: A site, facility, laboratory, company or other portion or subset of a Program Office/Departmental Element. Usually the portion or subset responsible for developing and maintaining the local security plan.

Security Clearance: An administrative determination that an individual is eligible for access to particular types or categories of classified information or material. (Security clearances indicate eligibility for access to Top Secret (TS), Secret (S) or Confidential (C).)

Safeguards and Security Information Management System (SSIMS): DOE's master repository for information regarding the status of safeguards and security findings and corrective actions and tracks facilities who possess nuclear material and/or have access to classified information. It contains current and historical DOE facility clearances, contracts, surveys, deviations to policy, incidents of security concern (IOSC) and other safeguards and security issues that require resolution at DOE and DOE contractor facilities. SSIMS is based on policy specified in DOE Order 470.1.

Security Repository: A place authorized for the storage of classified information. It may also be referred to as a safe, security container, vault or vault-type-room (VTR).

Technical Surveillance Countermeasures Operations Manager (TSCMOM): An optional title for an individual who functions as a TSCMOM in the Technical Security Program.