



PERFORMANCE DOCUMENT COVER PAGE

NOTE: If the following document is printed, this cover page must be attached to the front and the required information filled in below.

Date Printed: _____ **Dates Rev. No. Checked:** _____

Document Number: _____ **Revision Number:** _____

Title: _____

Person Checking Revision Number: _____

The attached document was printed from the online Performance Document System. The user must check that the hard copy revision number matches the revision number of the controlled document in the online Performance Document System. For future use, confirm the revision number's accuracy online and record dates that the revision number was checked.

Section Below Completed by the Performance Document Group Only

Document Type: Administrative Technical Emergency
 Standard Practice Alarm Response

Required Review Date: _____ Date Required Review Completed: _____

Document Status: Maintain As Is Revise Delete

If "Maintain As Is," Next Required Review Date: _____

If "Revise" or "Delete," Due Date: _____



OWNER: Security and Emergency Management	PPD-SE-1405	REVISION: 7
SUBJECT MATTER AREA: Classified Matter	PREPARER: Jamie Johnson	Page 1 of 40
PROCESS/PROGRAM DESCRIPTION	CONCURRENCE/DATE: Linda B. Raulston [Approval Signature on File]	3/20/18
TITLE: ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	APPROVED BY/DATE: Ed Dietrich [Approval Signature on File]	3/14/18
USQD <input checked="" type="checkbox"/> UCD <input type="checkbox"/> CAT X <input type="checkbox"/> EXEMPT <input type="checkbox"/>	EFFECTIVE DATE:	4/2/18
USQD/UCD/CAT X No: PSW-MS-PPDSE1405-1366	REQUIRED REVIEW DATE:	4/2/21
Exhibit L Mandatory Contractor Document No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>	If an Interim Document, Expiration Date:	

This document is approved for public release per review by:

Teresa D. Fancher 2/12/18

UCOR Classification Date

Information and Control Office

REVISION LOG			
Revision	Effective Date	Description of Changes	Pages Affected
7	4/2/18	Intent change. This revision addresses closure of issue IF-2018-0061.	4-6, 11-16, 21, 22, 32, 33, 38
6	4/24/17	Non-intent change. Extended a sentence in Section 5.3.3 Hand-Carrying Classified Matter, that the Secret Address Label will serve as the record of classified matter to be hand carried.	20
5	4/3/17	Non-Intent change. Added approval from the ODFSA as required by DOE O 471.6, Admin. Chg. 2 for Hand-Carry procedures. Removed incorrect reference to Email Recipients since emailing classified is prohibited. Updated Classified Mailstop list to remove mailroom.	4, 18, 19
4	8/30/16	Intent change. Complete rewrite. This revision addresses closure of issue IF-2016-0487.	All
3	5/21/15	Non-intent change. Updated signature page to reflect current UCOR approvers.	9
2	4/15/14	Non-intent changes. Title change from "Security Operations Manager" to "Security and Emergency Services Manager". Removal of CMPC staff names. Revised phone numbers.	All
1	2/20/13	Non-intent changes. Remove reference to Y-12 destruction and revise/change DOE Order number.	All
0	9/24/12	Initial issue.	All

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 2 of 40

PREFACE4

1. INTRODUCTION5

 1.1 PURPOSE.....5

 1.2 APPLICABILITY5

 1.3 REFERENCES5

 1.4 OTHER DOCUMENTS NEEDED5

2. ROLES AND RESPONSIBILITIES7

 2.1 UCOR SECURITY AND EMERGENCY SERVICES MANAGER SHALL:.....7

 2.2 UCOR PROJECT MANAGERS Shall:.....7

 2.3 UCOR PROJECT SERVICES AND SUPPORT MANAGER SHALL:8

 2.4 CLASSIFIED MATTER PROTECTION AND CONTROL PERSONNEL SHALL:8

 2.5 CLASSIFIED REPOSITORY CUSTODIAN SHALL:8

 2.6 PERFORMING WORK FOR UCOR THROUGH SUBCONTRACTORS OR SUB-TIER CONTRACTORS9

3. GENERAL PROVISIONS10

 3.1 TRAINING10

 3.2 ACCESS AUTHORIZATION.....10

 3.2.1 LEVELS AND CATEGORIES OF CLASSIFIED MATTER..... 10

 3.2.2 INCIDENTS OF SECURITY CONCERN (IOSC)..... 11

 3.3 CHANGES IN EMPLOYEE STATUS12

4. PROTECTING AND MARKING CLASSIFIED MATTER.....13

 4.1 GENERAL CLASSIFICATION REQUIREMENTS.....13

 4.1.1 CLASSIFICATION AUTHORITY 14

 4.1.2 DECLASSIFICATION AUTHORITY 14

 4.2 CLASSIFICATION CHANGES14

 4.2.1 DECLASSIFICATION AND REDACTION ACTIONS 14

 4.2.2 DOWNGRADE A DOCUMENT 15

 4.2.3 FOR OTHER SITUATIONS..... 15

 4.3 ACCOUNTABILITY15

 4.4 CLASSIFICATION DOCUMENT MARKING REQUIREMENTS.....15

 4.4.1 BASIC MARKING EXAMPLES 16

 4.5 WORKING PAPERS AND DRAFTS.....17

 4.6 COVER SHEETS18

 4.7 REMARKING CLASSIFIED DOCUMENTS.....18

 4.7.1 GENERAL 18

 4.7.2 OBSOLETE MARKINGS 18

 4.7.3 OTHER GOVERNMENT AGENCY DOCUMENTS NOT CONFORMING TO DOE REQUIREMENTS 19

5. TRANSMISSION OF CLASSIFIED MATTER.....20

 5.1 GENERAL.....20

 5.1.1 ELECTRONIC MAIL (E-MAIL) 20

 5.1.2 FACSIMILES..... 20

 5.2 UCOR MAIL SYSTEMS20

 5.2.1 CLASSIFIED MAIL STOPS 21

 5.3 TRANSMITTING CLASSIFIED MATTER INTERNALLY WITHIN THE ORR.....21

 5.3.1 TRANSMITTAL DOCUMENTS 21

 5.3.2 MAILING CLASSIFIED MATTER..... 22

 5.3.3 HAND CARRYING CLASSIFIED MATTER..... 22

 5.4 TRANSMITTING CLASSIFIED MATTER OUTSIDE THE ORR.....23

 5.4.1 MAILING CLASSIFIED MATTER..... 23

 5.4.2 HAND CARRYING CLASSIFIED MATTER..... 23

 5.4.3 RETURNING CLASSIFIED MATTER TO ETTP 24

 5.5 RECEIVING CLASSIFIED MATTER.....24

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 3 of 40

5.6	SHIPPING CLASSIFIED MATTER	24
5.6.1	COMMERCIAL EXPRESS SERVICE (OVERNIGHT)	24
6.	SECURITY REPOSITORIES AND STORAGE	25
6.1	GENERAL	25
6.2	REDUCTION OF HOLDINGS	25
6.3	APPROVAL FOR USE	26
6.4	COMBINATIONS	26
6.5	REQUIRED DOCUMENTATION	27
6.6	RELOCATION, TRANSFER, MAINTENANCE AND DEACTIVATION.....	28
6.6.1	MAINTENANCE AND REPAIR	28
6.7	EMERGENCY PROCEDURES.....	28
6.8	MEDICAL EMERGENCY SITUATIONS	29
7.	REPRODUCTION OF CLASSIFIED DOCUMENTS	30
7.1	GENERAL.....	30
8.	DESTRUCTION OF CLASSIFIED MATTER	31
8.1	GENERAL.....	31
8.2	ACCOUNTABLE CLASSIFIED MATTER.....	31
Attachment A	ACRONYMS/DEFINITIONS.....	32
Attachment B	DOCUMENT UNDERGOING CLASSIFICATION REVIEW COVER SHEET	38
Attachment C	DOE SF-700, SECURITY CONTAINER INFORMATION.....	39
Attachment D	DOE SF-702, SECURITY CONTAINER CHECK SHEET.....	40

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 4 of 40

PREFACE

This manual is applicable to all URS | CH2M Oak Ridge LLC (UCOR) individuals, and all individuals performing work for UCOR through subcontractor or sub-tier contractors, who are responsible for and use classified matter. Individuals involved in classified work must become familiar with the requirements contained herein. Supervision is responsible for ensuring that individuals under their direction are adequately trained and informed to prevent mishandling or compromise of classified matter.

Revisions, additions, deletions, or corrections to this manual are the responsibility of the Classified Matter Protection and Control (CMPC) Manager. Requests for changes should be identified in writing to the CMPC Manager.

The requirements in this document are in accordance with U.S. Department of Energy (DOE) Order (O) 471.6, *Information Security*, and DOE O 475.2B, *Identifying Classified Information*.

This document contains procedures for hand-carrying classified matter. Procedures for hand-carry must be approved by the Officially Designated Security Authority (ODSA) in accordance with DOE O 471.6. At this time there isn't an appointed ODSA, therefore the Officially Designated Federal Security Authority (ODFSA) must approve this document.

Jamie Johnson
UCOR CMPC Lead

Date

Ed Dietrich
Security and Emergency Services Manager

Date

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 5 of 40

1. INTRODUCTION

1.1 PURPOSE

This Manual provides the requirements for the safeguard and control of classified matter. It is developed and maintained by Classified Matter Protection and Control (CMPC) Personnel Jamie Johnson and Paula Woods. For information relating to this Manual please contact them at the following:

- Jamie Johnson - 865-241-5291
- Paula Woods - 865-576-1485

1.2 APPLICABILITY

This manual is applicable to all URS | CH2M Oak Ridge LLC (UCOR) individuals, and all individuals performing work for UCOR through subcontractor or sub-tier contractors, who are responsible for and use classified matter. Individuals involved in classified work must become familiar with the requirements contained herein. Supervision is responsible for ensuring that individuals under their direction are adequately trained and informed to prevent mishandling or compromise of classified matter.

1.3 REFERENCES

- Atomic Energy Act of 1954
- Executive Order 13526
- DOE O 471.6, *Information Security*
- 10 Code of Federal Regulations 1045 and DOE 475.2B

1.4 OTHER DOCUMENTS NEEDED

- DOE Standard Form (SF) 312, Classified Information Non-Disclosure Agreement (CMPC will provide the SF-312 forms as needed)
- DOE SF-700, Security Container Information Form (See Attachment C) (CMPC will provide the SF-700 forms as needed)
- DOE SF-702, Security Container Check Sheet (See Attachment D)
- DOE SF-703, Top Secret Cover Sheet (Contact CMPC to obtain all types of cover sheets)
- DOE SF-704, Secret Cover Sheet
- DOE SF-705, Confidential Cover Sheet
- MMCP11-00NSS-01, East Tennessee Technology Park Boundary for National Security Systems (available through UCOR Information Technology Organization)
- Form-123, Termination and Transfer Checklist
- Form-326, Authority to Transport Classified Matter Outside the Oak Ridge Reservation
- Form-367, Classified Document Receipt
- Form-531, Confidential Envelope (16 X 19) (Contact CMPC to obtain Confidential Envelopes)
- Form-532, Confidential Envelope (10 X 13)
- Form-533, Secret Envelope (12 X 16) (Contact CMPC to obtain Secret Envelopes)
- Form-534, Secret Envelope (10 X 13)

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 6 of 40

- Form-537, Data Transmittal
- Form-655, Subcontractor Staff Augmentation Employee Release Checklist
- Form-662, Security Package Address Label
- Form-1043, Maintenance Record for Security Containers, Vaults/Vault-type Room Doors

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 7 of 40

2. ROLES AND RESPONSIBILITIES

2.1 UCOR SECURITY AND EMERGENCY SERVICES MANAGER SHALL:

1. Serve as the UCOR official responsible for the overall management of the U.S. Department of Energy (DOE) CMPC Program for UCOR.
2. Ensure the necessary support and resources are provided for Security to conduct an effective CMPC Program in compliance with DOE orders and UCOR directives.
3. Include CMPC in UCOR's protection program planning documents.
4. Review and approve requested deviations and exceptions to this procedure.
5. Ensure that UCOR policies and procedures are developed and approved in accordance with applicable DOE orders.
6. Ensure that PPD-SE-1405 is included in the Mandatory Subcontractor Procedures list in the Proforma and other UCOR subcontractor directives.
7. Assure that organizations that handle or maintain classified matter adhere to all program requirements.
8. Interpret and approve UCOR CMPC policies and procedures in accordance with applicable DOE orders and directives.
9. Serve as the UCOR representative for resolution of any CMPC matters between the DOE Oak Ridge Office (ORO), UCOR, and the CMPC and Incidents of Security Concern (IOSC) contractor.
10. Appoint CMPC Point of Contact.

2.2 UCOR PROJECT MANAGERS SHALL:

1. Promote compliance with the UCOR CMPC Program.
2. Ensure that an action plan is established for all identified CMPC assessment deficiencies, and that these identified deficiencies are promptly corrected to meet program requirements.
3. Ensure that all organizational employees are scheduled for, receive, and remain current in the appropriate CMPC Training and/or briefings prior to handling classified matter.
4. Ensure that documented procedures for activities not specifically addressed in this manual are established and approved by the UCOR Security and Emergency Services Manager before program initiation and that these programs are reviewed annually.
5. Ensure that any organizational deviations or exceptions from the requirements in this manual (which must be approved by the UCOR Security and Emergency Services Manager) are maintained for easy retrieval.
6. Ensure that new activities are reviewed to determine if the work being performed is classified and requires material and document control, and ensure that the UCOR Security and Emergency Services Manager is included in new program planning.
7. Serve as the liaison for and provide oversight to the organization's CMPC Program when deemed appropriate for the organization.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 8 of 40

2.3 UCOR PROJECT SERVICES AND SUPPORT MANAGER SHALL:

Ensure UCOR subcontractors and sub-tier personnel are provided access to this procedure, and comply with the requirements provided therein.

2.4 CLASSIFIED MATTER PROTECTION AND CONTROL PERSONNEL SHALL:

1. Represent the UCOR Security and Emergency Services Manager concerning CMPC issues and resolutions, serve as the appointed CMPC Point of Contact.
2. Serve as the East Tennessee Technology Park (ETTP) Subject Matter Expert for the CMPC Program.
3. Review, interpret, and comment on new or revised DOE orders and directives.
4. Review, comment, and sign site security plans relative to CMPC requirements.
5. Develop and provide CMPC Training.
6. Develop and disseminate periodic awareness information.
7. Conduct CMPC self-assessments.
8. Assist DOE survey teams and other agency assessments.
9. Develop corrective action plans for identified assessment findings.
10. Serve as the liaison between UCOR Security Management and field personnel for CMPC issues and concerns.

2.5 CLASSIFIED REPOSITORY CUSTODIAN SHALL:

1. Ensure implementation of all CMPC requirements pertaining to their organization.
2. Serve as the primary point of contact for their organizational CMPC issues.
3. Ensure a reliable flow of information and guidance is disseminated to individuals within their organization.
4. Ensure all deficiencies identified in UCOR CMPC Self-Assessment are resolved and corrective actions implemented.
5. Contact CMPC personnel to request changes or deletions to the repository custodians.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 9 of 40

2.6 PERFORMING WORK FOR UCOR THROUGH SUBCONTRACTORS OR SUB-TIER CONTRACTORS

UCOR individuals and all individuals performing work for UCOR through subcontractors or sub-tier contractors shall:

- 1.** Follow all CMPC requirements stated in this Manual and any internal CMPC operating procedures.
- 2.** Successfully complete appropriate CMPC training.
- 3.** Immediately report known or suspected incidents of compromise of classified to IOOSC staff or Park Shift Superintendent (PSS) personnel via secure communication.

3. GENERAL PROVISIONS

3.1 TRAINING

UCOR employees and all UCOR subcontractors through sub-tier contractor personnel who have an L or Q clearance **must** successfully complete UCOR CMPC Training Module 6033. If comprehensive CMPC Training (equivalent to UCOR CMPC Module 6033) is successfully completed at the work site location, UCOR will accept this training as meeting the requirement for this module.

The training will be completed annually through the UCOR LEARN system.

3.2 ACCESS AUTHORIZATION

Access authorization is an administrative determination that an individual who is a DOE employee or a DOE contractor is eligible for access to classified matter.

Access to classified matter is granted only to persons who possess the appropriate security clearance (Q or L) and who require the matter in the performance of official duties or contractual obligations on a need-to-know basis.

Table 1 reflects the level and category of matter that may be accessed by an individual based upon clearance level.

Table 1: Level and Category of Matter

Classification	NSI	FRD	RD	TFNI
Top Secret	Q	Q	Q	Q
Secret	Q&L	Q&L	Q	Q&L
Confidential	Q&L	Q&L	Q&L	Q&L

3.2.1 LEVELS AND CATEGORIES OF CLASSIFIED MATTER

Levels of Classified Matter/Information:

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

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 11 of 40

Categories of Classified Matter/Information:

- Restricted Data (RD) – All data concerning: the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, except for data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act.
- Formerly Restricted Data (FRD) – Classified information removed from the RD category under the Atomic Energy Act (section 142(d)), after DOE and U.S. Department of Defense jointly determine it is related primarily to the military utilization of nuclear weapons and that the information can be adequately protected in a manner similar to NSI.
- National Security Information (NSI) – Information that has been determined pursuant to Executive Order (E.O.) 13526 or prior or successor E.O.s to require protection against unauthorized disclosure and is marked to indicate its classification status.
- Transclassified Foreign Nuclear Information (TFNI) – Information concerning the nuclear energy programs of other nations (including subnational groups) that was removed from the RD category under the Atomic Energy Act, (section 142(e)) after DOE and the Director of National Intelligence (DNI) jointly determine it is necessary to carry out intelligence-related activities under the National Security Act of 1947, as amended, and that the information can be adequately protected in a manner similar to NSI. This includes information removed from the RD category by past agreements between DOE and the Director of Central Intelligence or past and future agreements with the DNI. TFNI does not include:
 1. RD or FRD concerning United Kingdom (U.K.) or Canadian programs;
 2. Any U.S. RD or FRD, including that which the U.S. has transmitted to other nations;
 3. Any evaluation of foreign information based on the use of U.S. RD or FRD unless also specifically transclassified to TFNI or any evaluation that could reveal such data concerning the U.S., U.K., or Canadian programs;
 4. Classified atomic energy information received from a foreign government pursuant to an agreement imposing security measures equivalent for those in effect for RD; or
 5. Classified information on the Tripartite Gas Centrifuge and its successor programs, including data on the gas centrifuge work of each of the participants.

3.2.2 INCIDENTS OF SECURITY CONCERN (IOSC)

Custodians and authorized users of classified matter are personally responsible for the protection and control of such matter. If the information is not protected in a manner that prohibits unauthorized access or the potential for unauthorized access an IOSC could occur.

The responsible individual for the occurrence of an IOSC could receive a security infraction for failing to comply with security requirements for the protection of classified matter. The nature and severity of the security infraction shall be considered in determining appropriate disciplinary action(s).

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 12 of 40

3.3 CHANGES IN EMPLOYEE STATUS

When an individual possessing a security clearance has their employment transferred or terminated, or upon the individual's death or non-duty status exceeding 90 days, the immediate supervisor must ensure:

1. Form-123, Termination and Transfer Checklist or Form-655, Subcontractor Staff Augmentation Employee Release Checklist, is completed.
2. All classified matter possessed by the transferred/terminated individual is transferred or reassigned.
3. Combinations for any classified repositories to which the individual had access are changed.

NOTE: Classified matter, including "extra copies," is the property of UCOR (including subcontractors and sub-tier contractors) and must not be removed from the employer's control by any departing individual.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 13 of 40

4. PROTECTING AND MARKING CLASSIFIED MATTER

4.1 GENERAL CLASSIFICATION REQUIREMENTS

When creating documents in a classified subject area, the originator must ensure that a Derivative Classifier (DC) reviews the document if it potentially contains classified information and determines its initial classification level and category or protect it at the highest level and category until the DC review is obtained. These documents must be marked as either “Draft” or “Working Paper” on the front cover until they are marked as final documents with all appropriate DC markings noted. Although draft/working papers are not required to be portion marked, the titles should be unclassified when possible and marked accordingly by placing a “U” before the title. Any new information added to the working/draft document must receive a subsequent review or continue to be protected at the highest level and category.

ETTP does not have the ability to generate, send or receive classified email.

Portion marking is required for all NSI matter dated after April 1, 1997. Documents containing RD or FRD are not required to be portion marked.

Classified matter must be reviewed and brought up to current marking standards whenever it is released by the current custodian or removed from storage and placed into use (including use as reference material).

Documents received from Other Government Agencies and Foreign Governments that have not been marked to conform to DOE requirements do not need to be re-marked.

When marking the level or category is not practical (e.g., equipment, part, etc.), written notification of the classification level must be furnished to all recipients. The wrapper or holder of the material should be marked appropriately.

When extracting text or figures from a classified document the resulting document is considered a new document. The new document requires review by a DC if the new document is intended to be classified. If the document is intended to be unclassified, it must undergo two reviews. The first review may be conducted by a DC or Derivative Declassifier (DD); the second review must be conducted by a DD.

The originator or originating group [individuals including direct management responsible for developing newly-created-media (NCM)] is responsible for:

1. arranging and providing NCM for each initial review;
2. assuring that the NCM is examined by an appropriately-qualified DC; and
3. assuring that required forms are filled out as appropriate for each review.

Refer to UCOR-4388, *UCOR-CICO Policy for Reviews of Newly-Created-Media, East Tennessee Technology Park, Oak Ridge Tennessee*, for additional information.

Before any information generated by or for the Federal Government (Government Information) is made accessible to the public (e.g., distributed outside of Federal Government controls), it must be reviewed by the Classification and Technical Information control offices responsible for controlling that information to ensure that it is not classified or controlled unclassified information.

Only the ETTP Classification and Information Control Office (CICO) is authorized to make final classification and Unclassified Controlled Nuclear Information decisions or approve the public release of media containing scientific, technical or operational information in ETTP classified subject areas (e.g., Gaseous Diffusion and Centrifuge). ETTP CICO is also responsible for the public release of media generated by UCOR and UCOR

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 14 of 40

subcontractors that contain other site information, but this requires concurrence of appropriate other-site Classification and Technical Information Offices before release.

Contact the ETTP CICO office at 865-241-5318 for questions concerning classification.

4.1.1 CLASSIFICATION AUTHORITY

DCs working in the field only have the authority to determine whether a document or matter contains classified information (derivatively classify) or upgrade documents or materials based on the use of Classification Guides and with the concurrence of the ETTP CICO. The ETTP DCs are only authorized to review and classify or upgrade ETTP matter. If the matter is generated by another facility, their cognizant classification authority must perform the review. Only members of the ETTP CICO are authorized to make final classification determinations.

A DC also must have the authority to derivatively classify documents or material within their programmatic jurisdiction as defined in their letters of appointment from the ETTP CICO. These authorities are assigned in the following subject areas:

- Gaseous Diffusion Technology
- Gas Centrifuge Technology
- Safeguards and Security

4.1.2 DECLASSIFICATION AUTHORITY

Derivative Declassifiers (DDs) have the authority to derivatively declassify or downgrade only documents or material originated by UCOR, associated subcontractors, or the predecessors of these organizations, as defined in their letters of appointment from the Director, Office of Classification, DOE-Headquarters. These authorities are assigned in the following area(s): Isotope Separation and Safeguards and Security.

DDs may declassify or downgrade documents and material only in the area(s) in which they have been delegated authority. Such decisions must be based on:

- Classification and/or declassification guidance;
- Guide to the Declassified Areas of Nuclear Energy Research; or
- Restricted Data Declassification Decisions 1946 to the Present (if no other specific guidance exists).

This authority does not allow DDs to classify, upgrade, or reclassify information, documents, or material. DDs retains their authority so long as they remain in their current position and satisfy the biennial training and testing requirements. The only authorized DDs assigned to ETTP are the members of the CICO.

4.2 CLASSIFICATION CHANGES

Contradictions between the classification marked on a document and the actual classification of the information contained in the document necessitate a change in the classification markings.

4.2.1 DECLASSIFICATION AND REDACTION ACTIONS

Two reviews are required to declassify RD/FRD documents, or NSI document without a specific declassification date or event.

Classified documents that are being reviewed to produce a redacted (unclassified) version, must also be reviewed by two individuals with authority in the subject area. The first review may be conducted by a DC or a DD; the second review must be conducted by a DD.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 15 of 40

4.2.2 DOWNGRADE A DOCUMENT

When the classification level or category of information contained in a document or materials is changed by classification guidance, the document may be downgraded, as appropriate. The downgrade can be accomplished after one review is completed by a DD.

4.2.3 FOR OTHER SITUATIONS

For any other type of classification markings change, coordinate with a DC and obtain approval by a DD in ETTP CICO.

4.3 ACCOUNTABILITY

ETTP does not possess accountable matter.

4.4 CLASSIFICATION DOCUMENT MARKING REQUIREMENTS

Classified matter must include proper and complete classification markings. Current classified documents must contain the following classification markings.

1. Classification level,
2. Classification category (if RD, FRD or TFNI),
3. Caveats and special control markings (when required),
4. Title/Subject marking,
5. Portion marking (for documents containing NSI or TFNI that does not contain RD or FRD),
6. Classification Authority Block (provided by the DC).

When information is prepared on classified systems, hard-copy output (which includes paper or media) must be marked as follows:

1. as a final document with the appropriate markings for the classification of the information as determined by a DC according to a classification review of the actual output or,
2. as a working paper to the accreditation level and category of the information system (see Section 4.5 of this chapter for additional requirements that apply, regarding draft and working papers).

Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD). Documents dated after 4-1-96, must be marked in accordance with directives in place at the time of origin or in accordance with the requirements contained in this Manual.

1. If there is a question about the classification level or category of a document, the document must be reviewed by a DC and re-marked (if necessary) to clearly indicate the level and category to ensure proper protection.
2. Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings including declassification on a date or event, classification authority, or classifier's name, should be reviewed by a DC to ensure the classification level and category are still correct and then remarked to bring them into conformance with current marking requirements. This must be done if the

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 16 of 40

document is active, or is to be transmitted outside the organization for other than official archiving purposes.

Please see the DOE CMPC Marking Resource that is always up-to-date for examples of marking classified documents:

<http://energy.gov/sites/prod/files/2017/06/f34/CMPC-Marking-Resource-with-Attachment-Jan-2017.pdf>

4.4.1 BASIC MARKING EXAMPLES

NSI Cover/Title or First Page	NSI Interior Pages	NSI Outside Back Page/Cover
<p>SECRET</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p>Derivative Declassifier review required prior to declassification</p> </div> <p>Classified by: <u>Name, Title, Organization</u> Derived from: <u>CG-SS-4 9/12/00, DOE OC</u> Declassify on: <u>20371231 (i.e., YYYYMMDD).</u></p> <p>SECRET</p>	<p>SECRET</p> <p><i>(All interior pages marked top and bottom)</i></p> <p>SECRET</p>	<p>SECRET</p> <p>SECRET</p>

RD/FRD Cover/Title or First Page	RD/FRD Interior Pages	RD/FRD Outside Back Page/Cover
<p>SECRET RD or FRD</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p>RESTRICTED DATA. This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to Administrative and Criminal Sanctions. OR FORMERLY RESTRICTED DATA. Unauthorized disclosure subject to Administrative and criminal sanctions. Handle as Restricted Data in Foreign Dissemination, Section 144.b, Atomic Energy Act of 1954.</p> </div> <p>Classified by: <u>Name, Title, Organization</u> Derived from: <u>TCG-BTS-2, 08/29/0, DOE OC</u></p> <p>SECRET RD or FRD</p>	<p>SECRET RD or FRD</p> <p><i>(All interior pages marked top and bottom)</i></p> <p>SECRET RD or FRD</p>	<p>SECRET RD or FRD</p> <p>SECRET RD or FRD</p>

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 17 of 40

4.5 WORKING PAPERS AND DRAFTS

1. Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document.
2. Hard copies of working papers and drafts must contain the following markings:
 - a. The date created.
 - b. The highest potential overall classification level of the draft or working paper must be marked at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest classification level of that page (including unclassified) or the overall classification of the document.
 - c. Any new information added to the working/draft document must receive a subsequent review or continue to be protected at system high.
 - d. The overall category (if RD or FRD) of the draft or working paper must be marked on the first page of text. The category marking is not required on draft and working paper interior pages that contain RD or FRD information.
 - e. The annotation “Working Paper” or “Draft” must be placed on the first page of text.
 - f. Any applicable caveats or special markings must be annotated on the first page of text.
 - g. Markings prescribed for a finished document must be applied when:
 - released by the originator outside the activity or office,

Example of Activity

When multiple organizations are involved with the same project or program, it is acceptable to distribute the classified working paper or draft within the involved organizations as long as the distribution is not outside UCOR.

- retained for more than 180 working days from the date of origin, or
 - filed permanently.
3. Classified documents that are updated on a frequent basis, commonly referred to as “living documents” (e.g., documents that are part of an ongoing experiment or study) may be considered as originating each date they are changed. To demonstrate that the “living document” is in fact being changed frequently, a sheet may be attached to the front of the document that gives the number of pages and the date of the last posting.
 4. When the classification of matter cannot be determined and information must be sent outside the office of origin to an appropriate official for a classification review and determination, it must be marked, “DRAFT – Not Reviewed for Classification.” In order to preclude marking every page of a document being transmitted for classification review, it should have a “Document Undergoing Classification Review” cover sheet (see Attachment B) that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.

Please contact CMPC for cover sheets and if you need further information or assistance in marking classified matter.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 18 of 40

4.6 COVER SHEETS

Standard Form (SF) cover sheets must be applied to all classified documents when they are removed from a secure storage repository. SF 704 is the Secret (Red) cover sheet; and SF 705 is the Confidential (Blue) cover sheet. Contact CMPC to obtain cover sheets.

The purpose of a cover sheet is to prevent unauthorized visual access and to serve as an immediate identification of the overall highest classification level of a document. When the document is smaller or larger than 8 ½" x 11", any type of color-coded form (blue for Confidential, red for Secret) indicating the overall highest classification level and preventing unauthorized visual access must be affixed to the front of the document to meet the requirement when the document is outside a vault, Vault-type Room (VTR), or classified repository.

To prevent unauthorized visual access, the appropriate classified cover sheet can be affixed to the back of any classified document containing text on the last page. This can also be accomplished by using a blank sheet of paper marked with the highest classification level at the top and bottom of the page.

4.7 REMARKING CLASSIFIED DOCUMENTS

4.7.1 GENERAL

When possible, avoid returning improperly marked transmitted classified documents. If a document is improperly marked, discuss the marking problems by secure telephone with the transmitting office, and attempt to resolve these issues. Sometimes it is critical to return the document, such as when it does not have classifier information. Marking errors such as the classification level being omitted on the back of the document would be considered minor and could be corrected at the receiving facility or organization.

1. If there is a question about the classification level or category of a document, the document should be reviewed by a DC and re-marked (if necessary) to clearly indicate the level and category to ensure proper protection.
2. Classified documents that lack markings indicating declassification on a date or event, classification authority, or classifier's name, should be reviewed by a DC and re-marked if necessary.

When classified documents become active, or are transmitted outside the organization for other than official archiving purposes, they must meet current classification marking requirements. For example, if a classified document is removed from a repository and taken to a meeting, that constitutes making the document active and all current marking requirements must be met.

When extracts or changes are made to existing documents, a new document must be created, reviewed by a DC or the UCOR Classification Office, and meet the current marking requirements for the highest classification.

4.7.2 OBSOLETE MARKINGS

Before using or distributing a document marked with the following obsolete markings, a DC must determine the classification status and mark the document accordingly. Pending review, documents must be handled and protected as C-NSI.

1. Restricted.

This is an obsolete U.S. classification marking used prior to 12/15/1953, identifying a security level less sensitive than Confidential. This marking is still used by some foreign governments and international organizations.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 19 of 40

2. Official Use Only.

The Atomic Energy Commission used this term between 7/18/1949 and 10/22/1951 as an equivalent to the term Restricted. This marking is now used to identify unclassified information that may be exempt from disclosure under the Freedom of Information Act.

4.7.3 OTHER GOVERNMENT AGENCY DOCUMENTS NOT CONFORMING TO DOE REQUIREMENTS

As a rule, documents received from other Government agencies that have not been marked to conform to DOE requirements need not be re-marked. However, at a minimum, all documents received must clearly indicate a classification level and category (if RD or FRD).

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 20 of 40

5. TRANSMISSION OF CLASSIFIED MATTER

5.1 GENERAL

The Oak Ridge Reservation (ORR) referred to in this Manual consists of the ETTP, Consolidated Nuclear Security Y-12, the Oak Ridge National Laboratory, National Nuclear Security Agency, ORO, and other approved off-site contractor and subcontractor facilities within the Oak Ridge area.

When a custodian relinquishes classified matter to another individual, regardless of the mode of transmission (i.e., mailing, hand carrying, or express delivery), that custodian must verify that the intended recipient meets the following criteria for the level and category of the classified information involved in the transmission:

1. Requires access to the information in the performance of official or contractual duties (need-to-know criterion);
2. Has an appropriate security clearance;
3. Has all required programmatic or special-access approval(s);
4. External recipients that have an existing classified mailing address (CMA) approved by DOE to receive classified mail. Classified mailing and shipping addresses must be verified through the DOE Safeguards and Security Information Management System, and are valid for 30 days from the date of validation;
5. Internal recipients that have an approved classified mail stop (reference Section 5.2.1 of this chapter).

All classified matter transmitted (mailed or hand carried) to ORO must be taken to the ORO Central Library, located in the Federal Office Building.

5.1.1 ELECTRONIC MAIL (E-MAIL)

Transmission of **classified** information via **UCOR e-mail** is **prohibited**.

5.1.2 FACSIMILES

Contact CMPC staff for classified faxing needs.

5.2 UCOR MAIL SYSTEMS

UCOR is responsible for the protection and delivery of classified mail between facilities, and to and from the United States Postal Service (USPS). Classified mail will be transported by appropriately cleared individuals who maintain constant physical control of the matter at all times.

Classified mail being delivered must be delivered to and from approved classified mail stops. UCOR Mail Services personnel shall not, under any circumstances, open classified mail packages.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 21 of 40

5.2.1 CLASSIFIED MAIL STOPS

Classified mail stops must be certified by CMPC staff to receive and send classified matter.

1. The classified mail stop must be located where continuous visual or physical controls are used to prevent any attempt to divert classified matter. Classified mail stops must be under the control of appropriately cleared personnel. The mail stop must be posted indicating the classified mail stop number and the requirement that all classified deliveries be hand carried to only those individuals listed on the authorization list (see Item 2 below).
2. A list of individuals must be posted at the certified classified mail stop which indicates:
 - Name of the company or organization
 - Employees' name, badge number, and current security clearance level
 - Building and room number.

Below is a list of approved UCOR classified mail stops.

Building	Room	Mail Stop	Custodian
K-1650	122A	7308	Teresa Fanher
1916-T2	312	7301	R.P. Prince

Mail stops receiving and sending classified matter may not be relocated without the prior approval of the CMPC staff.

If classified mail should no longer be received or transmitted from a classified mail stop, the custodian must notify the CMPC staff.

5.3 TRANSMITTING CLASSIFIED MATTER INTERNALLY WITHIN THE ORR

5.3.1 TRANSMITTAL DOCUMENTS

The first page of a transmittal document must be marked with the highest classification level and category of the information contained in the transmittal and attachments. A transmittal might be classified and its classification might impact the markings (a secret transmittal with a confidential document) of classified information being transmitted, and with an appropriate notation to indicate its classification when the enclosures are removed. Additional markings (including category if RD or FRD) from the enclosure must be included on transmittal documents when they convey restrictions.

Please see the DOE CMPC Marking Resource that is always up-to-date for examples of marking transmittal documents:

<http://energy.gov/sites/prod/files/2017/06/f34/CMPC-Marking-Resource-with-Attachment-Jan-2017.pdf>

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 22 of 40

5.3.2 MAILING CLASSIFIED MATTER

Classified matter must be transmitted only in the performance of official and contractual duties. CMPC is the point of contact for all classified mailings into and out of ETTP. CMPC staff will ensure that appropriate document receipts are used, the package is properly marked and wrapped, and the appropriate mail carrier is used. The sender of classified matter is responsible for ensuring that the matter is properly marked with the appropriate classification markings.

5.3.3 HAND CARRYING CLASSIFIED MATTER

Any individual who possesses the need to know, a clearance appropriate to the level and category of matter being transported, and is traveling in the course of official company business is authorized to hand carry classified matter. This person must maintain positive control to prevent unauthorized access to the classified matter at all times.

When hand carrying classified matter within the ORR, and to/from a Property Protection Area (PPA) to/from a Limited Area (LA) within ETTP, double wrapping is required. The following double-wrap methods are acceptable:

1. Using a locked briefcase as the outer wrapping:

Confidential matter shall be placed inside a Confidential (blue) mail envelope. The envelope must indicate the names and addresses of both the sender and the receiver, and any applicable caveats.

Secret matter will be placed in a Secret (Red) Mail Envelope or placed in an appropriately marked envelope. One copy of a Secret Package Address Label (Form-662) will be completed, indicating the highest classification category and the recipient's and sender's classified mail stop, and any applicable caveats; and will serve as the record/receipt of classified matter. The completed Secret Package Address Label shall be placed on the outside front of the appropriately marked box or envelope. If using the internal Secret envelope, the completed Secret Package Address Label is placed in the plastic pouch on the outside of the Secret envelope.

The appropriately completed classified mail envelope will then be placed inside a locked briefcase. The briefcase must be of a solid construction with lockable hardware, and locked when transporting to/from PPA to/from a LA within ETTP. The briefcase must have a label attached identifying the sender's name and the UCOR CMA:

URS | CH2M Oak Ridge LLC
 East Tennessee Technology Park
 Security Organization, Bldg. K-1650, MS 7308
 Post Office Box 4699
 Oak Ridge, TN 37831-7308

The completed label attached to the briefcase indicating the sender's CMA furnishes the necessary address information for the outside wrapping requirement. There shall be no markings on the outside of the briefcase to indicate that the contents contain classified matter. The locked briefcase must remain attended at all times by an individual possessing the appropriate security clearance and meeting the need-to-know criterion for the contents being transported, or be secured in a repository approved for storage of classified matter.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 23 of 40

2. Using Two Opaque Envelopes

The classified matter is placed in the appropriately completed classified envelope and transported to ETTP CMPC for preparation as external mailing. If transporting from or through a PPA to ETTP CMPC, compliance is required for double wrapping using a locked briefcase as the outer wrapping.

ETTP CMPC will wrap the classified matter in two opaque envelopes as prescribed for mailing outside the ORR by using the USPS. The inner envelope must clearly identify the highest overall classification level, and category (if RD or FRD), of the contents, and any appropriate warning notices.

When two opaque envelopes are used for double wrapping, the classified matter shall be protected from direct contact with the inner envelope. This requirement may be accomplished by attaching the appropriate cover sheet to the front and back of the document.

The outer envelope will contain no markings to indicate classified matter is being transported. Both the inner and outer envelope will be appropriately sealed and addressed to the recipient's approved CMA. The CMA must be verified by UCOR Security (Classification Office) prior to mailing. Outer envelopes need no postage but must be marked "Return Postage Guaranteed."

The envelopes must remain attended at all times by an individual possessing the appropriate security clearance and meeting the need-to-know criterion for the contents being transported, or be secured in a repository approved for storage of classified matter.

The requirements for hand carrying classified matter within the ETTP are dependent upon whether the custodian is (or is not) relinquishing custodianship of the matter. The requirements for each scenario are provided below.

3. Hand Carrying Classified Matter **Within ETTP** *Without Relinquishing Custodianship*

If the owner of classified matter is not relinquishing custodianship by leaving it with a recipient (i.e., hand carrying the document or material to a meeting), and returning the matter to the same classified repository, the classified mailing envelope must indicate the owner's complete name and address.

4. Hand Carrying Classified Matter **Within ETTP** and *Relinquishing Custodianship*

If the owner of classified matter is relinquishing custodianship by leaving it with a recipient, the classified mailing envelope must indicate the owner's and recipient's complete name and address.

5.4 TRANSMITTING CLASSIFIED MATTER OUTSIDE THE ORR

5.4.1 MAILING CLASSIFIED MATTER

ETTP CICO will process all classified matter to be mailed outside the ORR. The custodian will double wrap the classified matter for transport to ETTP CICO as described in Section 5.3.3.

5.4.2 HAND CARRYING CLASSIFIED MATTER

Hand carrying classified matter for a meeting or for a visit **outside** of the ORR is discouraged. If the need to hand carry classified matter outside the ORR arises, contact CMPC.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 24 of 40

5.4.3 RETURNING CLASSIFIED MATTER TO ETTP

Contact CMPC when returning classified matter to ETTP. Classified matter returned to UCOR shall be mailed, unless absolutely unavoidable. If the matter must be returned with the traveler, Form-326, Authority to Transport Classified Matter Outside the Oak Ridge Reservation, is prepared prior to departure and must provide for the return trip to UCOR.

5.5 RECEIVING CLASSIFIED MATTER

Classified mail received from facilities outside the ORR must be sent to the UCOR CMA. A custodian who receives classified matter directly to their office address from external sources, regardless of the type of mail system, must keep the envelope(s) and wrapping(s) in which the matter was mailed, and shall notify the CMPC staff.

If classified matter is received in envelopes or wrappers that show evidence of tampering, the recipient must not open the package, but rather hold the package in the condition received and immediately notify the CMPC staff.

5.6 SHIPPING CLASSIFIED MATTER

Classified matter shall be shipped only through authorized package delivery systems and only to certified delivery areas. When classified matter is shipped outside UCOR facilities, only authorized means of shipment through DOE-approved shipping channels shall be used. ETTP CICO must be contacted to obtain the approved Classified Shipping Address.

5.6.1 COMMERCIAL EXPRESS SERVICE (OVERNIGHT)

The use of commercial express service organizations for transmitting classified matter is restricted to extreme emergency situations and the matter must be delivered to and secured at the receiving location the next calendar day. Contact the CMPC staff if express mail is required to transmit classified matter.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 25 of 40

6. SECURITY REPOSITORIES AND STORAGE

6.1 GENERAL

1. Custodians of classified repositories are responsible for both the containers assigned to them and the protection and control of such matter, to include proper storage.
2. Security containers shall not bear any external classification or other type markings that would indicate the level of classified matter authorized to be stored within the container. For identification, each security container shall bear an assigned number on the external portion of the classified repository.
3. Security containers and VTRs must be kept locked when not under direct supervision of an authorized individual.
4. Money, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft must not be stored in security containers that are used to store classified matter.
5. A minimum number of authorized persons shall have the combination to the storage container.
6. Classified matter that is not in use and under the control of an authorized person must be stored:
 - a. Inside a General Services Administration (GSA)-approved security container (repository) inside a LA or higher; or
 - b. Inside a locked vault/VTR within a LA or Exclusion Area equipped with an intrusion detection system or protective force response within 30 minutes of alarm annunciation.
7. The storage of classified matter outside of an approved security container must be authorized by the UCOR Physical Security Department and control of this type of storage (e.g., Non-conforming, Open Storage, or Permanent Burial) is described in separate and individual security plans.
8. Secret, Confidential, and Unclassified documents may be commingled in the same classified repository. For example, Secret, Confidential, and Unclassified documents may be stored in the same file folder.

NOTE: If using the preprinted and striped Confidential or Secret folders, be sure the folder does not state on the front, “Confidential Material Only” or “Secret Material Only,” when commingling these documents. The preprinted folders can still be used by marking out the “Only” after the “Confidential Material” or “Secret Material.” The preprinted folders must have the highest classification level marked top and bottom (front and back).

6.2 REDUCTION OF HOLDINGS

Throughout the year, classified document holdings must be reduced to the absolute minimum consistent with operational requirements. Organizations must routinely review their document holdings to determine if a reduction of classified holdings can be accomplished either through declassification, archiving or destruction. Multiple copies and obsolete matter should be destroyed as soon as practical to reduce classified inventories.

Documents not needed in daily activities should be prepared for storage and forwarded to the UCOR Inactive Records for archiving. Documents that no longer need to be retained must be destroyed in accordance with this Manual.

Contact CMPC for assistance with consolidation and preparing documents for archiving or destruction.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 26 of 40

Documents being prepared for retention must be coordinated with UCOR Inactive Records.

6.3 APPROVAL FOR USE

To obtain approval to use a repository for classified storage, a request must be submitted to CMPC.

6.4 COMBINATIONS

1. Change of Combination

If a combination change is required, the current custodian of the repository must submit a written request via email to the CMPC staff requesting the change. CMPC staff will submit a Maintenance Job Request through the BigFoot system for the locksmith to change the combination.

Combinations must be changed by authorized locksmiths. Combinations shall be changed at the earliest practical time after the following events:

- Initial receipt of a GSA-approved security container or lock.
- Reassignment, transfer, or termination of employment of any person having knowledge of the combination; when the access authorization granted to any such person is downgraded to a level lower than the category of matter stored; or when the access authorization has been administratively terminated, suspended, or revoked.
- Compromise or suspected compromise of a security container or its combination, or discovery of a security container unlocked and unattended.

2. Obtaining Combinations

The SF-700 form is provided by CMPC (See Attachment C). The locksmith assigns a randomly generated combination to each repository. Part 1 of the SF-700 form is completed by the custodian and the locksmith signs the form. Part 1 of the form is detached and stored inside the drawer of the repository. The combination is recorded on Part 2A of the SF-700 form by the locksmith. Part 2A is detached and placed inside Part 2 (envelope), sealed, and delivered to CMPC to be stored in the CMPC repository.

The repository custodians are responsible for the dissemination and protection of the classified combination.

3. Records of Combinations

Maintaining records of combinations is discouraged. If organizational needs dictate the need for combination lists, they must be protected at the highest level and category of matter stored in the container. If written or typed lists of combinations are maintained, they must be properly marked (including the DC markings), maintained as formal classified documents, and protected by the need to know in approved storage for classified matter. A sealed classified envelope annotated, "To Be Opened By Addressee Only," must be used to store classified repository combinations to meet the need-to-know criterion.

Custodians may recover changed or forgotten combinations by contacting CMCP staff.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 27 of 40

6.5 REQUIRED DOCUMENTATION

1. SF-700, Security Container Information Form (See Attachment C) is provided by CMPC.

Vaults and Vault-Type Rooms

- Part 1 of the SF-700 must be affixed to the inside of the door containing the combination lock.
- All personnel who have authority to open the VTR, shall be listed on the SF-700 and the personnel access list on file with the PSS.

Repositories

An SF-700 shall be completed for all security containers, rooms, vaults, and other approved locations for the storage of classified matter.

Part 1 of the SF-700 must be completed and placed inside the locking drawer. The form must be affixed to the back side of the front portion of the locking drawer.

Each of the following items must be completed on Part 1 of the SF-700:

- Area (i.e., LA, Protected Area, etc.)
- Building
- Room
- Organization
- Container number
- Manufacturer and class of container
- Manufacturer and lock model
- Date of combination change
- Print name/organization with signature of person making change

2. SF-702, Security Container Check Sheet (See Attachment D) is provided by CMPC.

SF-702 shall be used to provide a record of the names and times of the people who have opened, closed, and checked a particular container or VTR.

The SF-702 must be maintained with each individual repository and entrance to a VTR that is used to store classified matter.

All classified repositories and VTRs that have been opened must be double checked at closure, the end of the day, or the end of a shift. The SF-702 must be annotated in the “checked by” column indicating the initials of the individual performing the double check and the time the double check was completed.

A double check requires that each drawer of the repository, the door to the vault, or the VTR door be pulled, and the dial spun to ensure the cabinet or door is secured and cannot be opened without the combination. **The area must also be checked** to ensure no classified matter has been left out and unsecured.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 28 of 40

If the individual performing the end-of-day/shift check finds the repository open, they must immediately notify the PSS Office and CMPC/IOSC staff via secure transmission. The repository must be continuously attended or secured. The contents shall be checked no later than the next workday. Security containers and VTRs that were left unsecured shall be inspected to determine if classified matter is missing. The IOSC Inquiry Official will initiate an inquiry and ensure proper reporting of the incident.

If the securing mechanisms on classified repositories are faulty, or if the drawers fail to secure, immediately secure the classified matter, and contact CMPC staff or the PSS Office.

Each SF-702 shall be maintained for three months (90 days) following the last entry on the form. Maintenance of this form is the responsibility of the custodian that owns the repository or VTR.

3. DO NOT RELOCATE Label

The “DO NOT RELOCATE” magnetic label is posted on the front of all classified repositories. The label serves as a reminder that classified repositories shall not be relocated without approval from CMPC.

6.6 RELOCATION, TRANSFER, MAINTENANCE AND DEACTIVATION

When a custodian determines that a repository is no longer needed for classified storage and wishes to excess the repository or physically relocate/transfer to new custodian, (e.g., an individual transfers to another organization or terminates employment), the custodian of record must submit a request in writing via e-mail to CMPC staff.

6.6.1 MAINTENANCE AND REPAIR

A maintenance record is kept inside each repository. Form-1043, Maintenance Record for Security Containers and Vault/Vault-Type Room Doors, is available on the UCOR Forms page.

The maintenance record shall be retained in the drawer containing the combination lock with the required SF-700. A history for each security container, describing damage sustained and repairs accomplished shall be retained by the repository custodian for the life of the security container.

Neutralization of lockouts or repair of any damage that affects the integrity of a security container approved for the storage of classified matter shall be accomplished only by appropriately cleared locksmiths.

If the repository cannot be repaired, it shall be declared unsuitable for use and must be declassified/deactivated.

6.7 EMERGENCY PROCEDURES

During life-threatening emergencies, the health and safety of personnel shall take precedence over the need to secure classified matter. When feasible, classified matter shall be secured in the same manner as at the end of the work shift. Security containers and VTRs that were left unsecured during an evacuation shall be inspected by the custodian upon return to the facility to determine if classified matter is missing, and the custodian shall immediately notify the IOSC Inquiry Official via secure communications.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 29 of 40

During times of scheduled drills being performed at ETTP, classified matter shall be secured in security repositories and VTRs, and where applicable, intrusion alarms shall be activated. These repositories and VTRs must be secured.

Emergency personnel (security, fire, etc.) securing the scene of an emergency situation are responsible for the protection of government assets, to include the protection of classified matter.

6.8 MEDICAL EMERGENCY SITUATIONS

Classified information may be provided to the attending cleared physician in a medical emergency when such information is essential for the treatment of the patient. In life-threatening situations where medical personnel are uncleared, the UCOR Security Officer will execute a SF-312, Classified Information Non-Disclosure Agreement, and submit a report of unauthorized disclosure in accordance with DOE requirements.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 30 of 40

7. REPRODUCTION OF CLASSIFIED DOCUMENTS

7.1 GENERAL

Reproduction of classified documents must be accomplished only on approved equipment under appropriate security conditions to preclude unauthorized access. Copy machines approved for classified reproduction are designated by signage and labels.

Copying machines used for classified reproduction must be approved through CMPC and UCOR Information Technology. The approved machines must be located in approved areas.

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.

The following conditions must be met to preclude unauthorized access to classified information during reproduction:

- Documents shall be reproduced by appropriately cleared authorized persons in accordance with the procedures identified in this chapter, who know the procedures for classified reproduction, and only in the performance of official and contractual duties.
- Classified reproduction must not be performed in the presence of inappropriately cleared individuals.
- Reproduction of classified documents must be limited to the absolute minimum number of copies operationally necessary, and any further reproduction limitations shown on the document.
- Unacceptable or excess copies must be destroyed as classified information by approved destruction methods.
- Following classified reproduction, the copier is checked to ensure that no classified waste is trapped in the machine.
- After copying is completed, run one blank copy through the machine and check the copy for images. If images are still present, continue to run blank copies until no images remain. Destroy the blank copies as classified waste.
- Check the copying area and the copy machine (copy plate and trays) to ensure no classified matter remains before leaving the machine.

Reproduced copies are subject to the same protection and control requirements as the original matter and should be marked as soon as possible.

If part of a document is reproduced to stand-alone or to be incorporated into another document, it must be reviewed by a DC.

Reproduction restrictions must not restrict the reproduction of documents to facilitate review for declassification. However, after such reviews, reproduced documents remaining classified must be destroyed in accordance with the destruction requirements contained in this current Manual.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 31 of 40

8. DESTRUCTION OF CLASSIFIED MATTER

8.1 GENERAL

When classified matter is no longer required for operational, research, or historical purposes, it should be destroyed or reviewed for declassification. Classified matter shall be destroyed using the following methods approved by the CMPC staff: shredding, burning, melting, chemical decomposition, pulverization, or burial. Classified matter **must** be destroyed by equipment that has been approved by the CMPC staff. The CMPC staff must review and place the necessary certification signage on equipment used to destroy classified matter.

Classified matter must be destroyed beyond recognition to preclude reconstruction of classified matter.

Electronic storage media (CDs, DVDs, typewriter ribbon, VHS Tapes, etc.) containing classified information must be destroyed using approved destruction equipment and methods. Contact CMPC to arrange destruction of electronic media.

The destruction of classified matter shall be accomplished by individuals having appropriate access authorization ("L" or "Q" clearance) commensurate with the classification of the matter to be destroyed.

Classified matter shall be destroyed in accordance with records disposition schedules, including National Archives and Records Administration, General Records Schedule, and DOE Records Schedules.

Crosscut shredders purchased after December 21, 2003, used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm in width by 5 mm in length.

Users of classified shredders must inspect the particulate output each time to ensure that the particulate size is no larger than 1mm x 5mm. Contact CMPC staff if the particulate output is larger than the stated size requirement.

After the classified matter has been shredded in compliance with the required particle size, the particle residue resulting from the approved shredding can be placed in regular trash or recycle bins.

8.2 ACCOUNTABLE CLASSIFIED MATTER

ETTP does not possess accountable classified matter at this time.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 32 of 40

**Attachment A
ACRONYMS/DEFINITIONS
Page 1 of 6**

ACCESS AUTHORIZATION (SECURITY CLEARANCE). An administrative determination that an individual is eligible for access to classified matter, or access to or control over special nuclear material.

L-Security Clearance. A type of access authorization granted by DOE indicating that the recipient is approved for access to the following levels of classified matter on a need-to-know basis: Confidential Restricted Data (C-RD), Secret Formerly Restricted Data (S-FRD), Confidential Formerly Restricted Data (C-FRD), Secret National Security Information (S-NSI), Confidential National Security Information (C-NSI), Secret Transclassified Foreign Nuclear Information (S-TFNI) and Confidential Transclassified Foreign Nuclear Information (C-TFNI).

Q-Security Clearance. A type of access authorization granted by DOE indicating that the recipient is approved for access to the following levels of classified matter on a need-to-know basis: Top Secret, Secret, and Confidential.

ACCOUNTABLE DOCUMENT. Classified documents that contain information required by DOE, contracts, or programmatic agreements to be maintained in a formal accountability system. Accountable documents include, but are not limited to, Top Secret, North Atlantic Treaty Organization (NATO), United Kingdom, Communications Security (COMSEC), and Sensitive Compartmented Information (SCI) documents. ETTP does not possess accountable documents.

ADMONITORY MARKINGS. Warning notices specifying the authority and penalties associated with the categories of classified information.

AUTHORIZED INDIVIDUAL. Any individual, employee, or subcontractor who has an appropriate security clearance level and a need to know concerning classified matter.

CERTIFIED MAIL STOP. A designated area within an organization that is certified through UCOR Security as a delivery/pickup point for classified matter.

CICO. Classified Information Control Office

CLASSIFICATION CATEGORY. The four categories of classified information are: RD, FRD, TFNI, or NSI.

CLASSIFICATION LEVEL. A designation assigned to specific elements of information based on the potential damage to national security if it were disclosed to unauthorized persons. The three classification levels (in descending order of potential damage) are Top Secret (TS), Secret (S), and Confidential (C).

CLASSIFIED DOCUMENT RECEIPT (Form-367). A form used to establish or to transfer accountability of classified documents, and as a record of transmittal for Secret information leaving the ORR.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 33 of 40

Attachment A
ACRONYMS/DEFINITIONS
Page 2 of 6

CLASSIFIED INFORMATION. Information that is classified by statute or Executive Order (E.O.), including:

- (1) Information classified as RD, FRD or TFNI under the Atomic Energy Act, or
- (2) Information determined to require protection against unauthorized disclosure under E.O. 13526 or prior or successor E.O.s.

CLASSIFIED MAILING ADDRESS (CMA). A mailing address, including zip code, authorized by DOE through the Safeguards and Security Information Management System (SSIMS) for which procedures for classified mail deliveries have been approved. SSIMS authorizations are valid for 30 days from the verification date.

CLASSIFIED MATTER. Any combination of documents and material containing classified information.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC). A security program that includes procedures, facilities, personnel, and equipment used to safeguard classified matter from unauthorized disclosure.

CLASSIFIED REPOSITORY. A General Services Administration (GSA)-approved container, vault, or vault-type room (VTR), approved through UCOR Security for the storage of classified matter.

CLASSIFIER. A generic term used to identify either an Original Classifier or a Derivative Classifier.

Original Classifier. An individual who is authorized by DOE to classify National Security Information by an original determination based on the Executive Order where no specific guidance exists.

Derivative Classifier. (Previously referred to as Authorized Derivative Classifier). An individual who is authorized by the UCOR Site Classification Officer to determine that documents and/or material are (a) unclassified or (b) classified as Restricted Data (RD), Formerly Restricted Data (FRD), or National Security Information (NSI) in accordance with existing guidance or source documents.

COMPROMISE. Disclosure of classified information to unauthorized person(s). (See Unauthorized Disclosure.)

CONFIDENTIAL (C). A classification level that is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

CONFIDENTIAL MAIL ENVELOPE (Form-532 and Form-531). Approved envelopes used for sending Confidential documents through a package delivery system. May also be used to hand carry Confidential matter within the ORR. Contact CMPC to obtain Confidential Mail Envelopes.

CONTROL STATION. A facility operated to maintain records and control classified matter (e.g., the receipt, transmission, accountability, and disposition of accountable classified matter). UCOR Site Document Management Centers and the UCOR Security (Classification Office) serve as the UCOR Control Stations.

COVER SHEET (Standard Forms SF 704 and 705). A standard form placed on the face of a classified document that serves as a shield to protect information from inadvertent visual disclosure and to alert the custodian that classified information is attached. Contact CMPC to obtain Cover Sheets.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 34 of 40

Attachment A
ACRONYMS/DEFINITIONS
Page 3 of 6

DATA TRANSMITTAL (Form-537). A form used in the transmission of classified information or material that requires a signature upon receipt and for which the use of other forms is not appropriate.

DC. Derivative Classifier

DECLASSIFIED DOCUMENT. A previously classified document that:

1. has been declassified by the appropriate authority, in accordance with approved guidance, and from which the classification markings have been removed or canceled (RD, FRD, and NSI documents).
2. is marked for declassification at a specific time or event and that time or event has passed and has been reviewed and confirmed by an individual authorized to declassify or downgrade documents (NSI documents only.)

DERIVATIVE DECLASSIFIER (DD). An individual authorized to declassify or downgrade documents or material in specified areas as allowed by his or her description of authority.

DNI. Director of National Intelligence

DOCUMENT CUSTODIAN. Any individual or an office to which a classified document is issued and who is responsible for the protection, handling, and marking of that document.

DOCUMENT NUMBER. An alphanumeric identifier assigned to a document to aid in the accountability, tracking, and transmission of classified matter.

DOE. U.S. Department of Energy

DOWNGRADE. A determination by an appropriate authority, at DOE Headquarters or with other agency coordination, that (1) information may be protected at a level lower than the current classification level or, at DOE or by contractor DD determine that (2) a document or material may be protected at a level and/or category lower than the marked classification level and/or category.

E.O. Executive Order

ETTP. East Tennessee Technology Park

EXCLUSION AREA. A type of DOE security area defined by physical barriers and subject to access control where mere presence in the area would result in access to classified information.

FACILITY. An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

FORMERLY RESTRICTED DATA (FRD). Classified information jointly determined by DOE or its predecessors and the Department of Defense to be related primarily to the military use of atomic weapons and removed by DOE from the RD category pursuant to Section 142(d) of the *Atomic Energy Act of 1954*, as amended, and safeguarded as NSI subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 35 of 40

Attachment A
ACRONYMS/DEFINITIONS
Page 4 of 6

GSA. General Services Administration

INACTIVE RECORDS CENTER. Document Management Center for interim storage of legacy records and for processing inactive records to disposition.

INCIDENT OF SECURITY CONCERN (IOSC). Events that cannot, at the time of occurrence, be determined to be an actual violation of law but that are of such significant concern to the DOE Safeguards and Security program as to warrant preliminary inquiry and subsequent reporting.

INFRACTION. DOE F 5639.3, *Report of Security Infraction*, form documents information relating to a security infraction and is issued through UCOR Security to individuals failing to comply with security requirements.

LIMITED DISSEMINATION. Restricted controls for classified information established by an original classification authority to emphasize need-to-know measures available within the regular security system.

LIMITED AREA (LA). A type of Security Area having boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized persons to classified matter or special nuclear material.

NATIONAL SECURITY INFORMATION (NSI). Any information that has been determined, pursuant to Executive Order 13526 or any predecessor order, to require protection against unauthorized disclosure and that is so designated. The levels TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information.

NCM. Newly-created-media

NEED TO KNOW. A determination by an authorized person having responsibility for classified matter that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function, perform tasks or services essential to the fulfillment of a classified contract or program, or to perform official or contractual duties of employment.

NONACCOUNTABLE DOCUMENTS. Classified documents, including Weapon Data, that are not required to be maintained in a formal document accountability system (see "Accountable Document").

O. Order

OAK RIDGE RESERVATION (ORR). ETTP, the Y-12 National Security Complex, the Oak Ridge National Laboratory, DOE ORO, National Nuclear Security Agency, and other approved off-site facilities within the Oak Ridge area.

ODSA. Officially Designated Security Authority

ORIGINATOR. The person who generates classified information in the form of a document (not the person who (only) prepared the master, determines the classification, approves the issuance, or effects the reproduction).

ORO. Oak Ridge Office

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 36 of 40

Attachment A
ACRONYMS/DEFINITIONS
Page 5 of 6

PORTION MARKING. The application of classification and control markings to individual parts (e.g., paragraphs, chapters, titles, figures) of a classified document to indicate their specific classification level (if NSI), classification level and category (if RD or FRD), or control category (e.g., Unclassified Controlled Nuclear Information [UCNI], Official Use Only [OUO]). [Note that portion marking of RD or FRD documents is discouraged at DOE.]

PROPERTY PROTECTION AREA (PPA). A type of Security Area having boundaries identified with barriers and access controls for the protection of DOE property.

PSS. Park Shift Superintendent

REPOSITORY CUSTODIAN. Any person who has responsibility for the proper use and maintenance of a classified repository and its contents.

RESTRICTED DATA (RD). All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the *Atomic Energy Act of 1954*, as amended.

SANITIZATION. The process of removing classified information from a document or classified automated information system.

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

SECRET MAIL ENVELOPE (Form-533 and 534). Approved envelopes used for sending Secret documents through a package delivery system. May also be used to hand carry Secret matter within the ORR. Contact CMPC or CICO to obtain Secret Mail Envelopes.

SECRET PACKAGE ADDRESS LABEL (Form-662). A label used in the internal mailing system for the transmission of nonaccountable Secret documents. The label is fully completed and placed in the transparent protector of the internal Secret mailing envelope.

SF. Standard Form developed by DOE.

SOURCE DOCUMENT. A classified document from which information is extracted and included in another document whose classification is derived from the classification markings of the individual portions from which the information was extracted.

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 Atomic Energy Act 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.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 37 of 40

Attachment A
ACRONYMS/DEFINITIONS
Page 6 of 6

TRANSMITTAL MARKINGS. Markings on a transmittal letter that identify the level and category of classified information involved in the transmittal and the classification of the transmittal letter when separated from the enclosures.

Top Secret (TS). Containing or being information whose unauthorized disclosure could result in exceptionally grave danger to the nation.

UNATTENDED MATTER. Classified matter that is not in the direct custody or control of an authorized employee having the appropriate access.

UNAUTHORIZED DISCLOSURE. A communication or physical transfer of classified information to an unauthorized recipient.

UNCLASSIFIED (U). (1) The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority; (2) a marking used to indicate that a declassified document, page or title of an RD, FRD, or NSI document, or portion of an NSI document is not sensitive or controlled.

UPGRADE. A determination by an appropriate authority (1) at DOE Headquarters that raises the classification level or category of information, or (2) at DOE or by contractor DC that raises the classification level or category of a document or material to protect the contents adequately, including the classification level and/or category of a document or material that was never marked as well as one erroneously marked as unclassified.

URS | CH2M OAK RIDGE LLC (UCOR) SECURITY AND EMERGENCY SERVICES MANAGER. UCOR individual responsible for the overall UCOR Security Program. This individual reports to the Environmental, Safety, and Health and Quality Assurance Manager, and serves as the Project Manager for Security.

USPS. United States Postal Service

VTR. Vault-Type Room

WEAPON DATA. RD or FRD concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

WORK FOR OTHERS. Research, development, testing, manufacturing, or experimentation operations and activities conducted at DOE facilities for a U.S. agency other than DOE.

WORKSHEETS. Notes, work papers, preliminary copies of pages of a document, and additional or revised pages before they are incorporated into a final copy. The life span of this draft information is limited to 180 days without classification review and transformation into a permanent document.

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 38 of 40

**Attachment B
DOCUMENT UNDERGOING CLASSIFICATION REVIEW COVER SHEET
Page 1 of 1**

BELOW IS AN EXAMPLE ONLY

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) ▼

NOTE: *National Security Information* documents should have only the estimated classification level circled.

FORMERLY RESTRICTED DATA

Unauthorized Disclosure Subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act 1964.

Instructions for Use of this Form

(You do not need to be an Derivative 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). **NOTE:** *National Security Information* documents should have only the estimated classification level circled.
3. Fill in "To," "From," and "Date" lines.
4. Place this Form on top of the document pending classification review, and place an appropriate coversheet (SF-703 for Top Secret, SF-704 for Secret, or SF-705 for Confidential) on top of this page.

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

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

TOP SECRET / SECRET / CONFIDENTIAL

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

OWNER: Security and Emergency Management	PPD-SE-1405
ETTP CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) MANUAL	REVISION: 7
	Page 39 of 40

**Attachment C
DOE SF-700, SECURITY CONTAINER INFORMATION
Page 1 of 1**

BELOW IS AN EXAMPLE ONLY

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PRIVACY ACT STATEMENT ON REVERS.	1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
	ETTP	K-1652	210
	4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)	5. CONTAINER NO.	
	SECURITY	K-SEC-1234	
	6. MFG & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
MOSLER/GSA	X09	00/00/0000	
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE			
Ima R. Locksmith			
10. Immediately notify one of the following persons if this container is found open and unattended.			
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE	
Ira M. Custodian	123 ABC Ave., Oak Ride, TN	482-1234	
Ura B. Alternate Custodian	234 CDE Ave., Oak Ridge, TN	482-2345	
Juan A. Moore Custodian	567 FGH Ave., Oak Ridge, TN	482-3456	
Repository Data Base Manager	K-1652, Room 210	241-5734	
1. ATTACH TO INSIDE OF CONTAINER	700-101 NSAI3540-01-214-5372	STANDARD FORM 700 (8-85) Prescribed by GSA/ISOO 32 CFR 2003	

