



UCOR

an Amentum-led partnership with Jacobs

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: _____



UCOR

an Amantum-led partnership with Jacobs

OWNER: Security and Emergency Services	PPD-SE-1415	REVISION: 4
SUBJECT MATTER AREA: Classification and Information Control	PREPARER: Leesa Laymance	Page 1 of 46
PROCESS/PROGRAM DESCRIPTION	CONCURRENCE/DATE: Linda B. Raulston 3/11/21 [Approval Signature on File]	
TITLE: ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	APPROVED BY/DATE: Edward Dietrich 3/11/21 [Approval Signature on File]	
USQD <input type="checkbox"/> UCD <input type="checkbox"/> CAT X <input checked="" type="checkbox"/> EXEMPT <input type="checkbox"/>	EFFECTIVE DATE: 3/15/21	
USQD/UCD/CAT X No: USQD-MS-CX-SECURITY-0193	REQUIRED REVIEW DATE: 3/15/24	
Exhibit L Mandatory Contractor Document: No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>	If an Interim Document, Expiration Date:	

- 1. INTRODUCTION3
 - 1.1 PROGRAM DEFINITION3
 - 1.2 POLICY BASIS FOR CUI PROGRAM3
- 2. RESPONSIBILITIES4
 - 2.1 UCOR SECURITY AND EMERGENCY SERVICES MANAGER4
 - 2.2 PROJECT SERVICES AND SUPPORT MANAGER4
 - 2.3 UCOR CUI PROGRAM MANAGER4
 - 2.4 DCs5
 - 2.5 UCNI ROs6
 - 2.6 UCOR AND SUBCONTRACTOR PERSONNEL6
 - 2.7 SUPERVISORS OF PERSONNEL POSSESSING CUI7
- 3. OVERVIEW OF CUI8
 - 3.1 PROTECTION OF CUI8
 - 3.2 IDENTIFICATION OF CUI8
 - 3.3 MARKING OF CUI9
 - 3.4 SECURING CUI9
- 4. OFFICIAL USE ONLY (OUO) INFORMATION11
 - 4.1 IDENTIFICATION OF OUO INFORMATION11
 - 4.2 MARKING REQUIREMENTS FOR MEDIA CONTAINING OUO INFORMATION15
 - 4.3 SECURING OUO17
- 5. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION22
 - 5.1 IDENTIFICATION OF UCNI22
 - 5.2 MARKING REQUIREMENTS FOR MEDIA CONTAINING UCNI23
 - 5.3 SECURING UCNI24
- 6. DOCUMENTS CONTAINING OUO AND UCNI29
 - 6.1 IDENTIFICATION29
 - 6.2 MARKING REQUIREMENTS29
 - 6.3 SECURING29
- 7. TRAINING30
 - 7.1 MODULE 19938, CUI TRAINING30
 - 7.2 MODULE 031302, ETTP UCNI REVIEWING OFFICIAL TRAINING30
- 8. CUI ASSESSMENT PROGRAM31
- 9. CHANGES IN PERSONNEL STATUS32
- 10. IOSC AND INFRACTIONS33
- 11. RECORDS34
- ATTACHMENT A DEFINITIONS/ACRONYMS35
- ATTACHMENT B EXAMPLE: OUO DOCUMENT38
- ATTACHMENT C EXAMPLE: UNCLASSIFIED HARD COPY MEMO TRANSMITTING OUO39

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 2 of 46

ATTACHMENT D	EXAMPLE: EMAIL CONTAINING OUO	40
ATTACHMENT E	EXAMPLE: NON-SENSITIVE EMAIL TRANSMITTING OFFICIAL USE ONLY	41
ATTACHMENT F	EXAMPLE: UCNI DOCUMENT	42
ATTACHMENT G	EXAMPLE: UNCLASSIFIED HARD COPY MEMO TRANSMITTING UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION	43
ATTACHMENT H	EXAMPLE: NON-SENSITIVE EMAIL CONTAINING UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION	44
ATTACHMENT I	EXAMPLE: NON-SENSITIVE EMAIL TRANSMITTING UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION	45
ATTACHMENT J	EXAMPLE: DOCUMENT CONTAINING BOTH UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI) AND OFFICIAL USE ONLY (OUO).....	46

This document is approved for public release per review by:

Teresa D. Fancher 8/29/17

UCOR Classification Date

Information and Control Office

REVISION LOG			
Revision	Effective Date	Description of Changes	Pages Affected
4	3/15/21	Intent change. Updated company name and logo. Corrected links in procedure.	1, 3, 20, 28
3	9/25/17	Intent change. The major changes include the following: 1) revision of how UCNI is allowed on UCOR AIS-certified computers and can be emailed with certain restrictions, 2) addition of attachments for UCNI examples, 3) clarification of DC, UCNI RO, and Personnel Responsibilities, and 4) minor revisions to include DOE-HQ comments.	All
2	11/17/14	Intent Change. Reformatted document. The major changes include the following: 1) Allow hand carry of OUO documents between or within a facility; 2) All personnel are required to take Module 19938, CUI Training; and 3) An addition method of encryption called Secure Email Gateway has been added. If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then, the sender can send the password in a separate email so that the recipient can access the file.	All
1	2/21/13	Non-Intent Change. Corrected numbering sequence within document.	All
0	1/31/13	Initial release. Replaces BJC-SE-1405, <i>Bechtel Jacobs Company, LLC (BJC) Information Security (INFOSEC) Manual, Part II (Rev. 6)</i> .	All

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 3 of 46

1. INTRODUCTION

1.1 PROGRAM DEFINITION

Controlled Unclassified Information (CUI) – formerly Unclassified Controlled Information (UCI) – CUI is unclassified government information requiring protection. It is data for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government, commercial, or private interests. The categories of CUI are Official Use Only (OUO) information and Unclassified Controlled Nuclear Information (UCNI). UCNI is nuclear-related information protected under the Atomic Energy Act (AEA).

It is the responsibility of each UCOR, an Amentum-led partnership with Jacobs, UCOR subcontractor, and UCOR sub-tier contractor personnel to protect CUI. The purpose of the UCOR CUI Program is to ensure the protection of CUI, at an appropriate level of risk, by these responsible parties. The Program is compliant with all applicable U.S. Department of Energy (DOE) Orders/Manuals and other statutory requirements.

The following paragraphs further define the Program and prescribe requirements for its implementation. Additional information can be obtained in the UCOR folder on the “Q” drive: Q:\Security\CUI_Shared\CUI. This folder provides CUI “Quick Reference Sheets,” examples, and other helpful reference tools. Questions concerning CUI requirements should be directed to the UCOR-Classification and Information Control Office (CICO) (referred to hereafter as CICO) staff.

1.2 POLICY BASIS FOR CUI PROGRAM

1.2.1 General DOE Policies

- 10 Code of Federal Regulations (CFR) Part 1017, Identification and Protections of Unclassified Controlled Nuclear Information. These regulations contain the majority of the requirements for implementing the UCNI program.
- DOE Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE Order 471.3, Administrative Change 1, *Identifying and Protecting Official Use Only Information*
- DOE Manual 471.3-1, Administrative Change 1, *Manual for Identifying and Protecting Official Use Only Information*

1.2.2 Related UCOR Policies

- UCOR-4388, *UCOR-CICO Policy for Reviews of Newly-Created-Media, East Tennessee Technology Park, Oak Ridge, Tennessee*
- PROC-SE-1005, *Classification and Information Control*

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 4 of 46

2. RESPONSIBILITIES

2.1 UCOR SECURITY AND EMERGENCY SERVICES MANAGER

The UCOR Security and Emergency Services Manager is the UCOR official responsible for the design, implementation and effectiveness of the UCOR CUI Program. Specific responsibilities include:

- Ensure CUI Program requirements are compliant with applicable DOE orders.
- Assure that CUI is handled in accordance with the UCOR CUI Program requirements and that CUI protection requirements are included in all UCOR protection program-planning documents.
- Approve any deviation from the requirements specified in this CUI manual.
- Ensure that sufficient resources are provided for effective program execution.

2.2 PROJECT SERVICES AND SUPPORT MANAGER

The Project Services and Support Manager shall ensure that all UCOR Subcontracts and sub-tier Contracts are compliant with the requirements of the UCOR CUI Program. Specific responsibility includes:

- Ensure that CUI Program requirements are incorporated in the Mandatory Subcontractor Procedures list in the Proforma.

2.3 UCOR CUI PROGRAM MANAGER

Definitions for Sections 2.3, 2.4, 2.5 and 2.6:

- (1) **CUI – formerly UCI** – Data for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government interests. Some of the elements of CUI include Applied Technology, Cooperative Research and Development Agreement Information, Export Controlled Information (ECI), Privacy Act (PA) Information, Proprietary Information (PI), and UCNI.
- (2) **CUI*** means CUI excluding UCNI and ECI (OUO, Exemption 3), but including OUO Exemptions 4, 5, 6, and 7.
- (3) **(3)STOI** means Scientific, Technical/Technological and Operational Information related to a classified subject matter area.
- (4) **(4)CI** means classified information.

The UCOR CUI Program Manager is the UCOR Classification Officer. This individual reports to the UCOR Security and Emergency Services Manager and is responsible for the effective and efficient management of the UCOR CUI Program. Specific responsibilities include:

- Represent the UCOR Security and Emergency Services Manager concerning CUI issues and resolutions.
- Serve as the UCOR point-of-contact for the UCOR CUI Program and Subject Matter Expert (SME) for the East Tennessee Technology Park (ETTP) CUI.
- Review, interpret and comment on new or revised DOE orders and directives.
- Maintain company-level CUI programmatic procedures and guidance documents that provide for a consistent implementation of the CUI program.
- Develop and conduct CUI performance assessments; evaluate UCOR/Subcontractor/Sub-tier contractor personnel for understanding of and capabilities to identify and secure CUI.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 5 of 46

- Review, comment and approve ETTP security plans concerning CUI requirements.
- Develop and provide CUI Training; Assure new personnel training adequately reflects UCOR CUI Program requirements.
- Develop and disseminate CUI awareness information. Assist DOE survey teams and other agency assessments. Develop corrective action plans for assessment issues.
- Provide definitive decision-making for CUI and review media potentially containing CUI for public release.
- Provide expert advice for CUI decision making to Derivative Classifiers (DCs), UCNI Reviewing Officials (ROs), and other personnel.
- Public release authority; CICO (or CICO-approved DC) guidance/approval required for STOI.

2.4 DCs

Specific constraints/responsibilities include:

- Definitive decision making that STOI is **not** CI//UCNI/ECI or that STOI is CI.

NOTE: If not *absolutely certain* that STOI is not CI/UCNI/ECI, then protect and for:

- CI: check with CICO before making a definitive decision (unless otherwise authorized by CICO).
 - UCNI: transfer information to an UCNI RO or CICO.
 - ECI: transfer information to CICO for definitive decision making.
- No public release of STOI without CICO guidance/approval, unless excepted by authority letter.
 - Definitive decision making for CUI*; if not absolutely sure about CUI*, then check with an SME (e.g., CICO or designated DC).
 - Provide expert advice for CUI* decision making to UCOR/Subcontractor/Sub-tier contractor personnel.
 - Assure that each individual within their area of responsibility (1) understands the procedures for review of information that has the potential to contain CI/CUI, (2) can identify information that is, or is potentially, CI/CUI, and (3) understands the requirements for securing CI/CUI.

2.4.1 DCs with Public Release Authority

Some DCs have been granted public release of STOI as stated in their authority letter. These DCs are noted on the DC List, which is provided on the Classification and Information Control Office home page.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 6 of 46

2.5 UCNI ROs

UCNI ROs are responsible for making definitive UCNI decisions and for providing expert advice concerning UCNI to individuals within their area of responsibilities. UCNI RO authority is discussed in Section 5.

- SME in their technical area of responsibility.
- Knowledgeable in sensitive government information (SGI) associated with those areas and capable of sound decision-making for technical SGI identification.
- Provide expert advice for implementing the CUI program within their area of responsibilities.

Specific responsibilities include:

- Definitive decision that STOI is **not** UCNI.

NOTE: If not *absolutely certain* that STOI is not UCNI, then check with CICO before making a definitive decision (unless otherwise authorized by CICO).

- No public release of STOI without CICO guidance/approval (unless otherwise authorized by CICO).
- Assure that each individual within their area of responsibility understands the procedures for review of information that has the potential to contain UCNI, can identify (potential) UCNI and understands the requirements for securing UCNI.

2.5.1 UCNI ROs with Public Release Authority

Some UCNI ROs (who are also DCs) have been granted public release of STOI by CICO as stated in their authority letter. If an UCNI RO does not have DC authority, then the UCNI RO should obtain the DC review before releasing to the public.

2.6 UCOR AND SUBCONTRACTOR PERSONNEL

Responsibilities include:

- Identifying information that is or is potentially CUI to which they have access or potential access, and securing that information in accordance with the requirements of this CUI Program.

NOTE: If not *absolutely certain* that STOI is not CI/UCNI/ECI, then protect and for:

- a. CI: transfer information to a DC or CICO for definitive decision making.
- b. UCNI: transfer information to an UCNI RO or CICO for definitive decision making.
- c. ECI: transfer information to CICO for definitive decision making.

- Definitive decision for CUI*; if not absolutely sure about CUI*, then check with a DC or a CUI* SME (e.g., CICO, UCOR Legal).
- No public release of STOI without approval by CICO or a CICO-authorized individual.
- Following all CUI requirements stated in this manual.
- Successfully completing Training Module 19938, “CUI Training,” and any appropriate CUI training as determined necessary by an Area Project Manager.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 7 of 46

- Immediately reporting known or suspected incidents of compromise of CUI to Cyber Security. Cyber Security will then notify the Incidents of Security Concern (IOSC) Inquiry Official (IO) as necessary. If an incident occurs outside of regular work hours, then notify the Park Shift Superintendent.

2.7 SUPERVISORS OF PERSONNEL POSSESSING CUI

- All CUI in the possession or custody of the person being transferred from or whose employment is being terminated with UCOR, UCOR subcontractor or sub-tier contractor are retrieved and transferred or reassigned. CUI, including “extra copies,” is the property of the site contractor and/or subcontractor, and must not be removed from the contractor's control by any departing, including terminated, individual.
- A Termination and Transfer Checklist (Form-123) for UCOR employees, or a Subcontractor Staff Augmentation Employee Release Checklist (Form-655) for Subcontractor/sub-tier employees is completed. All required items listed on the form must be completed.
- No CUI is left unattended or abandoned.
- Assure that each person within their area of supervision can and does protect CUI according to this procedure.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 8 of 46

3. OVERVIEW OF CUI

3.1 PROTECTION OF CUI

The protection of CUI requires three activities: (a) the identification of information that is CUI, (b) the marking of media that contains CUI, and (c) the securing of the media. The term “media” is used to indicate those entities that convey information. Examples of media are: hardcopy documents, electronic files, electronic disks/chips, videos, emails, phone conversations, equipment, and the knowledge (i.e., information) held by an individual. Securing CUI means controlling access to those entities.

For the purpose of securing CUI, it is useful to divide media into three categories: (a) physical media, (b) electronic media, and (c) human beings. Even though CUI may reside in various categories of media and be transferred from one category to another, it must be protected as long as it exists. *For physical or electronic media*, this means from its incorporation in through the destruction of the media in which it resides. *For human beings*, it means a continuing control by the use of “need to know.”

It may occur that information once considered CUI is no longer CUI in which case protection is no longer required and any marking of media containing CUI should be removed. For UCNI, this determination is made by an UCNI RO. For OUO, refer to Section 4.2.5.

3.2 IDENTIFICATION OF CUI

The identification of CUI requires a reasonably clear definition of what is and is not CUI and then using/interpreting that definition to make a prudent decision about whether information is CUI.

3.2.1 Defining CUI

At ETTP, there are two categories of CUI: OUO information and UCNI.

OUO Information is information that may be exempted from public release by the Freedom of Information Act (FOIA). Types of OUO information relevant to ETTP are:

- Statutory Information (e.g., Export Controlled Information) [Exemption 3],
- Commercial/Proprietary Information [Exemption 4],
- Privileged Information (e.g., DOE decision making information) [Exemption 5],
- Personal Privacy Information [**protected** personally identifiable information—(PII)]-including Privacy Act information [Exemption 6], and
- Law Enforcement Information [e.g., sensitive security-related and Operations Security (OPSEC) information] [Exemption 7].

UCNI means certain unclassified Government information concerning nuclear facilities, materials, weapons, and components whose dissemination is controlled under section 148 of the AEA and 10 CFR 1017. At ETTP, UCNI is typically technical information associated with classified subject areas (e.g., Gaseous Diffusion or Centrifuge, but not Security).

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 9 of 46

3.2.2 Reviewing for CUI

Before any information generated by or for the Federal Government (Government Information) which has the potential to be CUI is distributed *outside the originating person/group*, that information must be reviewed for the presence of CUI (OUO and UCNI). DCs review for OUO and potential UCNI and UCNI ROs review for UCNI. If the DC determines that there is information that is potentially UCNI, then an UCNI RO review must also be performed. If the information contains STOI, then a DC (or CICO) review is required. If the information is potentially CUI* only, then the originator can perform the review, although it is strongly suggested that if uncertainty exists then the information should be examined by a DC or CICO. It is important when CUI is present that the media containing the CUI be marked properly; checking with a DC is recommended.

Unless approved by CICO, no potentially-CUI STOI (UCNI/ECI) may be released outside of government controls (public release) without CICO authorization. For further information on the development of new documents, refer to UCOR-4388, *UCOR-CICO Policy for Reviews of Newly-Created-Media, East Tennessee Technology Park, Oak Ridge, Tennessee*. Because UCOR manages programs at other sites [i.e., Oak Ridge National Laboratory (ORNL) and Y-12 National Security Complex (Y-12)], STOI associated with these sites must be reviewed by a DC/UCNI RO certified by the site. This review is sufficient for the limited/internal distribution of STOI. If the STOI is being reviewed for public release, then both (a) CICO **and** (b) the ORNL and Y-12 Classification Offices (whichever is appropriate) must perform the DC-UCNI RO review, and the Y-12 Information Release Office or the ORNL Technical Information Office (whichever is appropriate) must determine if the information is OUO. CICO can facilitate these reviews by either performing them (with agreement from the other sites) or by transferring media to the appropriate site reviewing entities.

3.3 MARKING OF CUI

Physical and electronic media that contain CUI must be marked to clearly identify the type of CUI in the media. How to mark media containing OUO information is discussed in Section 4. UCNI markings are discussed in Section 5.

3.4 SECURING CUI

Securing CUI means denying unauthorized access to that information.

Granting Access. A person granted routine access to CUI must have a need to know the specific information in the performance of official or contractual duties. Because CUI is unclassified, a security clearance (“L” or “Q”) is not required; however, recipients must be advised of the protection requirements. An individual who is in possession of CUI and grants routine access to individuals that are not UCOR or UCOR subcontractors shall notify each person granted such access of the applicable CUI requirements. Providing a copy of this procedure to the individual is adequate notification. Refer to Section 4 for specific access requirements for OUO. Refer to Section 5 for specific access requirements for access to UCNI.

Denying Access. It is the responsibility of each UCOR/subcontractor personnel to secure CUI against unauthorized access. **Information that may be CUI must be secured until discussed with or reviewed by a DC or CICO.** It is useful to think about securing/denying access to CUI in terms of common activities associated with the handling of information: (a) Use, (b) Reproduction, (c) Storage, (d) Transmission (inside and outside of DOE controls), and (e) Destruction. Each activity has associated with it protocols for securing CUI which means in general securing the media in which CUI resides. The protocols for securing media containing CUI will be discussed in detail in Sections 4 (OUO) and 5 (UCNI).

An Important Consideration. Personal devices are becoming more common at UCOR and, although there are areas where they are restricted from being used, they have become valuable tools to help ensure work is performed **safely**. Although they can be very useful, remember that these tools have the ability to back up

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 10 of 46

information to the cloud, which is, essentially, setting them up for public release. When you use your personal devices to create data of or about the site, ensure you are protecting that information in accordance with all UCOR procedures; this includes sending it only over UCOR-approved email methods, deleting data after it has been transferred to UCOR, and/or removing it from your device. Data can take many forms, such as voice recordings, photos, videos, emails, and notes. It is your responsibility to protect all UCOR information, no matter what form it takes or how it was created.

Decision Making Assistance. DCs in your organization and CICO are a useful reference for questions about CUI issues. The current list of DCs is provided on the Classification and Information Control Office home page. The current list of CICO staff members is also provided [on the Classification and Information Control Office home page](#). It is important to note that STOI that may be ECI must be secured and transferred to CICO for decision making.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 11 of 46

4. OFFICIAL USE ONLY (OUO) INFORMATION

4.1 IDENTIFICATION OF OUO INFORMATION

4.1.1 How to Determine the Presence of OUO Information

Does the information:

1. Have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.
2. Fall under at least one of five FOIA exemptions (exemptions 3 through 7).

NOTE: Information cannot be controlled as OUO unless (a) OUO Guidance applies, or (b) both of the criteria in 1) and 2) above are met.

With the exception of sensitive safeguards and security information (OUO, Exemption 7) as determined primarily by CG-SS-5, there is very little specific written guidance to assist in OUO decision making. In general, personnel who are uncertain whether or not media contains OUO information should consult their assigned DC or CICO for assistance or a definitive determination (CICO).

4.1.2 How to Determine When Information is No Longer Considered OUO Information

CICO makes the final determination whether or not media previously marked as containing OUO information still contains OUO information. Until that determination is made, the media marked as OUO must continue to be handled as OUO.

4.1.3 OUO FOIA Exemptions

Circumvention of Statute, Exemption 2

Previous to June 1, 2011, sensitive security information was marked as OUO Exemption 2. POL-4 advised that information previously considered as Exemption 2 should now be identified as Exemption 7, Law Enforcement, if still applicable. Examples of this type of information are provided under Exemption 7 of this section.

Statutory Exemption, Exemption 3

Exemption 3, Statutory Exemption, protects information, the disclosure of which is specifically protected by law and is not otherwise controlled.

Examples of statutory exemptions include:

- Federal Technology Transfer Act allows Federal agencies to protect for 5 years any commercial and business confidential information that results from a Cooperative Research and Development Agreement with a non-Federal party
- Procurement Integrity Act – Source selection information
- Internal Revenue Code – Taxpayer identification numbers
- Patent Act – Applications for patents
- Arms Export Control Act – Information pertaining to license applications under the Act (ECI)

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 12 of 46

- Export Administration Act – Information pertaining to license applications under the Act (ECI)
- National Security Act of 1947 – Intelligence sources and methods
- Espionage Act – Information pertaining to communication intelligence and cryptographic devices
- Nuclear Non-Proliferation Act of 1978 (ECI)

The primary type of information protected by Exemption 3 at ETTP is ECI. ECI is a category of information DOE established as a nonproliferation tool. It is defined as unclassified technical information by whose distribution is subject to export control and whose unrestricted public dissemination could provide significant assistance to proliferants or potential adversaries of the United States.

ECI at ETTP is Sensitive Nuclear Technology, defined to be any information which is not available to the public and which is important to the design, construction, fabrication, operation, or maintenance of a uranium enrichment or nuclear fuel reprocessing facility or a facility for the production of heavy water, but shall not include Restricted Data controlled pursuant to chapter 12 of the AEA. This includes equipment on the Commerce Nuclear Suppliers Group Dual-Use List and Trigger List.

Sound ECI decision making requires strong technical subject matter expertise in the development and implementation of the Sensitive Nuclear Technology. For that reason, media containing STOI that has the potential to be ECI *must be referred to CICO for definitive decision making.*

Commercial/Proprietary, Exemption 4

Exemption 4 information encompasses:

1. Trade Secrets – A trade secret is “a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.” Trade secrets are often technical in nature.
2. Commercial or Financial Information – Information that is (a) commercial or financial, (b) obtained from a person (includes corporations), and (c) privileged or confidential. Commercial or financial information is usually not technical in nature.

Examples of Commercial/Proprietary include:

- Trade secret information (e.g., Coca Cola formula)
- Commercial or financial information, such as income, profits, losses, costs, in connection with bids, contracts (solicited/unsolicited) or proposals and other related information received in confidence
- Customer/supplier lists
- Government credit card or bank account numbers
- Security measures for commercial entities performing work for the Government

The following two factors should be considered when deciding whether information may be OOU under Exemption 4:

1. Could cause damage to the business entity associated with the information or negatively affect DOE program effectiveness or contractor relationships
2. Would impair the Government’s ability to obtain information in the future

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 13 of 46

Privileged Information, Exemption 5

Although there are many categories of privileged information, the privilege most likely to be used within DOE is the deliberative process privilege (also known as “executive privilege”). This privilege ensures that Agency staff is free to make candid comments in the formulation of Agency policies and plans.

Examples of Privileged Information include:

- Draft or final documents that contain advice, opinions or recommendations on new or revised Government decisions and policies, regardless of whether prepared by Federal personnel, contractors, consultants, etc.
- Evaluations of contractor personnel and their products and services by DOE personnel.
- Information of a speculative, tentative or evaluative nature concerning proposed plans to procure, lease or otherwise acquire and dispose of materials, real estate, facilities, or functions when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

The following factors should be considered when deciding whether information is OOU under Exemption 5:

1. The information must be for inter-agency or intra-agency communication only. This means that any document not generated for public release may be considered an inter-agency or intra-agency document.
2. Release of the document could cause harm to the process of developing Agency policy because such release could:
 - a. Discourage open, frank discussions concerning draft policies;
 - b. Cause premature disclosure of proposed policies before they are finally adopted; and
 - c. Cause confusion in the public that could result from disclosing reasons and rationales that were not ultimately the grounds for an Agency’s action.

Personal Privacy, Exemption 6

Personal Privacy information (PPI) is personal information associated with a specific individual (or individuals) [Personally-Identifiable Information (PII)] that, if disclosed, could reasonably be expected to cause damage to the individuals concerned (e.g., personal distress or embarrassment or could lead to identity theft).

Examples of PPII include PII for which the government has responsibility:

- Personal details about an individual (e.g., social security number, citizenship data, date of birth).
- Intimate details of an individual’s life (e.g., marital status, religious affiliation, sexual orientation or associations, medical conditions, criminal history, financial data).
- Personnel matters in which administrative action, including disciplinary action, may be taken.
- Evaluation of candidates for employment or security clearances.
- Performance appraisal/evaluation reports.

In general, PII that directly concerns UCOR operations (employee number, job descriptions, work location, work phone number) does not require protection and is not PPII.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 14 of 46

Privacy Act information is PPII protected by the Privacy Act. Privacy Act Information is protected as OUO Exemption 6 information; however, there are specific requirements in addition to the Exemption 6 requirements as defined by DOE O 206.1.

Law Enforcement, Exemption 7

At ETTP, Exemption 7 applies to Safeguards and Security Information. This information could potentially damage the safety/security of governmental interests or persons at or near the DOE site. This information is specified either by CG-SS-5 or as an OPSEC concern based on local security expertise.

Examples of security-related OUO which is based on topical guidance (i.e., CG-SS-5) include:

- Vulnerability assessments.
- Agency computer access codes.
- Information concerning critical systems, facilities, stockpiles, or other assets subject to harm.
- Details of security systems.

Examples of security-related information that may be OUO Exemption 7 based on security expertise:

1. Information that provides consequences of malevolent acts or location of Special Nuclear Material.
 - a. Nuclear safety information included in Documented Safety Analysis, Hazard Assessment Documents, Safety Analysis Documents, criticality documents, etc.
 - b. Emergency Management information included in Emergency Planning Hazard Analyses, Emergency Action Levels, and Emergency Planning Zone.
2. Maps/Drawings that provide interior features for certain facilities.
3. Text that discusses any historical process in the building or facility or specific uses of chemical or substances in the building or facility.
4. Information regarding the current location of significant quantities of chemicals or radiological or hazardous substances that could be dispersed and could cause significant harm to persons at the site.
5. Information that relates the existence of environmental contamination to a specific facility/facilities.
6. Information regarding the exact location of any current fissile material deposits (e.g. in equipment) or in material storage areas.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 15 of 46

4.2 MARKING REQUIREMENTS FOR MEDIA CONTAINING OUO INFORMATION

4.2.1 General OUO Marking Requirements Hard Copy and Electronic Documents

Any unclassified document or material that has been reviewed and determined to contain OUO information shall be marked on the front of the document or material as follows.

<p>OFFICIAL USE ONLY</p> <p>May be exempt from public release under the Freedom of Information Act (5 USC 552), exemption number and category:</p> <p>_____</p> <p>Dept. of Energy review required prior to public release.</p> <p>Name/Org: _____ Date: _____</p> <p>Guidance, if applicable: _____</p>

The following marking, “**OFFICIAL USE ONLY**,” shall be placed on the bottom of the face of the document and (1) on the bottom of each interior page of the document, or, if more convenient, (2) on the bottom of only the interior pages that actually contain OUO (markings should be clearly visible). The “**OFFICIAL USE ONLY**” marking is recommended on the bottom of the back page, but this is not a requirement.

Although not a requirement, an OUO cover sheet can be attached to the front of the OUO document to provide basic requirements. The OUO cover sheet (Form-1152) is available on the UCOR Forms page.

Attachment B shows an example of an OUO document indicating the correct markings.

4.2.2 Special Markings

In addition to the general OUO markings, if a document contains a) ECI, b) PI, or c) PA Information, the bottom portion of the front page of the OUO document must be marked with an appropriate admonitory marking in addition to the general OUO markings (markings should be clearly visible). If a document has PA and ECI, then both admonitory markings must appear on the front page of the OUO document in addition to the general OUO markings.

4.2.2.1 ECI Admonitory Marking Requirement

The admonitory marking for ECI is the following:

EXPORT CONTROLLED INFORMATION

Contains technical data whose export is restricted by _____. Violations may result in administrative, civil, or criminal penalties. Limit dissemination to U.S. Department of Energy and major U.S. DOE contractors. The cognizant program manager must approve other dissemination. This notice shall not be separated from the attached document.

Reviewer

Date

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 16 of 46

4.2.2.2 PI Admonitory Marking Requirement

The admonitory marking for PI is the following:

PROPRIETARY INFORMATION

This technical data contains proprietary data furnished under Contract No. XXXXXX (insert correct contract number) with the U.S. Department of Energy. Disclosure outside the government is not authorized without prior approval of the originator, or in accordance with provisions of 48 CFR 952.227 and 5 U.S.C. 552.

4.2.2.3 PA Admonitory Marking Requirement

The admonitory marking for PA is the following:

PRIVACY ACT RECORDS

RESTRICTIONS ON DISCLOSURE – This record contains personal/confidential medical information and is subject to protection by the Privacy Act of 1974; 5 U.S.C. & 552 (a). Federal or contractor employees who willfully make an unauthorized disclosure of information from this record shall be guilty of a misdemeanor and fined up to \$5,000.

4.2.3 Marking Special Format Media

Special format media include photographs, viewgraphs, films, magnetic tapes, disks, audiotapes, videotapes, DVDs, etc. If possible, the special format documents must be marked in a manner consistent with documents (front marking and page marking). If space is limited, page marking is sufficient (Official Use Only or OUO).

4.2.4 Marking Documents Maintained In Restricted Access Files

Documents that contain or may contain OUO information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. However, a document removed from these Restricted Access Files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked. (**NOTE:** Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.

4.2.5 Removal of OUO Markings

Markings Applied Based on Guidance. OUO markings applied based on guidance may be removed by any personnel when the guidance used to make the determination states that the information is no longer OUO. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OUO. Once those deficiencies have been corrected, the OUO marking may be removed.)

Markings Applied Based on Employee's Evaluation. OUO markings applied based on an employee's evaluation may be removed by (1) the employee who initially applied the marking, (2) the supervisor of the

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 17 of 46

employee who initially applied the marking, (3) a FOIA authorizing official who approves the release of the document in response to a request made under FOIA, or (4) CICO.

Markings applied based on Guidance or criteria stated in Section 4.1.1: After it has been confirmed that no OOU exists in the document, then a) the general OOU markings and any additional markings need to be marked out, and b) place the following marking on the bottom of the front of the document:

<p>DOES NOT CONTAIN OFFICIAL USE ONLY INFORMATION</p> <p>Name/Org. _ Date: _</p>
--

4.2.6 Media with Obsolete Markings

Documents dated prior to December 15, 1953, and marked as “Restricted” and documents dated from July 18, 1949, through October 22, 1951, and marked as “Official Use Only” must be reviewed by a Derivative Declassifier or a Derivative Classifier (single review only). Until the review is completed, such documents ***must be handled and protected as Confidential National Security Information*** pending a determination of their proper classification and unclassified sensitivity.

4.3 SECURING OOU

Information generated by or for the Federal Government (Government Information) and identified by any UCOR/Subcontractor personnel as OOU must be secured in accordance with the requirements of this manual.

4.3.1 Physical Media

Physical control shall be maintained over any physical media (e.g., paper documents, materials and physical/electronic equipment) marked as containing OOU so as to prevent unauthorized access to the information.

4.3.1.1 In Use

An authorized individual shall maintain physical control over any document, material or equipment in use that is identified as containing OOU to prevent unauthorized disclosure. In the case of a hard-copy document, care must be taken that the contents cannot be viewed by an individual without an appropriate need to know.

4.3.1.2 Reproduction

OOU may be reproduced without permission of the originator. Reproduction shall be limited to the minimum number of copies necessary consistent with the need to carry out official duties. Reproduced copies shall be marked and protected in the same manner as the original document. Copy machine malfunctions must be cleared with all paper paths checked for OOU material. Care must be taken that the contents cannot be viewed during reproduction by an individual without an appropriate need to know.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 18 of 46

4.3.1.3 In Storage

When unattended, OOU documents shall be stored in the following manner.

1. **On-Site.** In the Limited Area when OOU documents, material or equipment are unattended, they may be stored with other unclassified matter in unlocked files, desks or similar containers. OOU must not be left where unauthorized visual access is granted (e.g., left on a desk in an unlocked office, placed on a bulletin board in general use areas, or left unattended at a common printer or copier).

In the property protection area (PPA) or General Access Area (GAA), when OOU documents, material or equipment are unattended, they shall be stored in a locked drawer, desk, file cabinet, or in a locked room.

2. **Off-Site.** In an area that is neither controlled nor guarded (i.e., a private residence or a subcontractor facility), OOU documents, material or equipment shall be stored in a locked container or behind a locked door where physical control over the document is maintained. OOU cannot be processed on a non-government approved computer.

4.3.1.4 Transmission

A document that (1) transmits an attachment or enclosure marked as containing OOU, and (2) does not itself contain OOU must be marked on the front or first page of the document as follows to call attention to the presence of OOU in the attachment(s) or enclosure(s):

<p>Document(s) Transmitted Contain(s) OOU Information</p>
--

The type of OOU (i.e., Exemption number and title as noted in Section 4.1.3) being transmitted must appear on the first page of the transmittal document to ensure adequate protection is afforded to the controlled information. For example, a non-sensitive transmittal document transmitting OOU would be marked **OFFICIAL USE ONLY** at the very bottom of the transmittal document and the statement “Document Transmitted Contains OOU” appears just above the bottom portion of the transmittal document. See Attachment C for an example.

The specific type of OOU being transmitted by any of the means described below, is *not* annotated on the outside of the opaque envelope. OOU or Official Use Only should not appear on the outside of the envelope.

4.3.1.4.1 Within the Oak Ridge Reservation (ORR)

Transmission shall be by means to preclude unauthorized disclosure or dissemination. A single, opaque envelope or wrapping must be used to transmit OOU within the ORR. The opaque envelope or wrapping must be sealed and marked “TO BE OPENED BY ADDRESSEE ONLY.”

4.3.1.4.2 Outside the ORR

Transmission by mail outside of the ORR is as follows.

1. A single, opaque envelope or wrapping must be used to transmit OOU outside the ORR. The opaque envelope or wrapping must be sealed and marked, TO BE OPENED BY ADDRESSEE ONLY.
2. Any of the following U.S. mail methods may be used: U.S. First Class, Express, Certified, or Registered Mail.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 19 of 46

3. Any commercial carrier using a signature service may be used.

4.3.1.4.3 Hand Carry Within or Outside the ORR

Authorized individuals (i.e., those who are granted access) shall hand-carry OOU document between or within a facility as long as the authorized individual carrying the document can control access to the document being transported. The transporter must meet the access requirements and maintain constant control and vigilance over the OOU matter. Visual access to the contents of the OOU document shall not be permitted during transit.

4.3.1.5 Destruction

Any document or material identified as containing OOU must be destroyed by using one of the following methods:

- Using a strip-cut shredder that produces strips no more than ¼-inch wide (ensure that strips do not contain printed text that can be read).
- Using a cross-cut shredder approved by the Classified Matter Protection and Control staff for classified destruction.

Personnel who remove OOU from the site must either return it to the site for proper storage and/or destruction or provide the OOU to an appropriately trained individual (with need-to-know) who knows how to handle, store and destroy OOU.

4.3.2 Electronic Media

Physical control shall be maintained over any electronic media (electronic disks/chips/cards, videos) marked as containing OOU so as to prevent unauthorized access to the information.

4.3.2.1 In Use and Reproduction

OOU may be processed only on an Automated Information System (AIS) certified computer/copier/fax or a subcontractor computer approved by a UCOR Information Technology (IT) security plan. AIS certified computer/copier/fax equipment will have a US DOE government sticker or IT sticker on each piece of equipment. An AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OOU information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

Personnel can use their home computer/laptop/electronic device to access OOU files that reside on the UCOR system. Personnel are not allowed to save any OOU files to their home computer or any other electronic device unless approved by UCOR IT.

4.3.2.2 In Storage

OOU is protected in electronic form (e.g., computer files) when it resides on the approved AIS network. An approved AIS network is a government-owned computer (i.e., has a US DOE sticker on it). Personnel must prevent access to OOU information stored on an approved computer by persons who do not require the information to perform their jobs or other DOE-authorized activities. This can be accomplished by using authentication, file access controls or passwords.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 20 of 46

4.3.2.3 Transmission of EMails

The specific type of OUO (as listed in Section 4.1.3) being transmitted electronically by any of the means described below, should *not* be annotated in the subject line. OUO or Official Use Only should not appear in the subject line of the email.

4.3.2.3.1 Within the UCOR Firewall (name@ettp.doe.gov)

When OUO is sent via electronic mail, insert “**OUO**” before text in the first line of the message. “**OUO**” is listed first when the email contains OUO.

If the message itself is not OUO, but an attachment contains OUO, the message must indicate that the attachment contains OUO. The attachment must have all required OUO markings. “**Document Transmitted Contains OUO Information**” should be listed as the first line of text in an email when the attachment contains OUO.

Examples of both an actual OUO email and a non-sensitive email transmitting OUO are shown in Attachment D and Attachment E, respectively.

4.3.2.3.2 Outside the UCOR Firewall

The email will be marked as noted in Section 4.3.2.3.1.

OUO (including protected PII) must be encrypted or password protected when emailed outside the UCOR firewall (email addresses other than name @ettp.doe.gov). Encryption can be accomplished by using one of the following methods: 1) Secure Email Gateway, 2) DOE Entrust Public Key Infrastructure, or 3) WinZip. Contact the UCOR Helpline (574-8000) for assistance with Secure Email Gateway (http://intranet.ettp.gov/IT/Help/pdf-docs/ETTP_MEG_Users.pdf), Entrust and WinZip.

If encryption is not available or some other form of protection is desired, the OUO information may be included in a Microsoft office file or Adobe PDF file that is protected by a password and attached to the email message. Then, the sender sends the password in a separate email so that the recipient can access the file.

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

4.3.2.4 Transmission by Telecommunications

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

When sending OUO by facsimile, the sender must contact the intended recipient to ensure an individual meeting the access requirements is ready to receive the transmission and that the fax is not left unattended. The sender is also responsible for making a follow-up phone call to the recipient to confirm that the entire OUO document was received, that the OUO is not left unattended on the fax machine, and that the faxed information is in the possession of authorized individual meeting the access requirements.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 21 of 46

4.3.2.5 Transmission over Voice Circuits

OUO information transmitted over voice circuits should be protected by encryption whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used. Hard-line telephone circuits are preferred over cell phone circuits when possible.

4.3.2.6 Destruction

AIS media containing OUO must be destroyed per instructions from UCOR IT Organization.

4.3.3 Human Beings

Basic idea is that: Knowledge that contains CUI must not be communicated to individuals who (1) do not have the need to know in order to perform government work or (2) have the need to know, but who may not protect the CUI appropriately.

Information is defined as facts, data, or knowledge itself regardless of the medium of its conveyance. (Documents are deemed to convey or contain information and are not considered information per se.) The transfer of information including voice (telephonic, point-to-point), narrative message, presentations, radio, and communications must consider and use the most secure means available. These considerations include ensuring personnel without a need-to-know do not overhear voice communications in any form and assuring before presentations/discussions that participants have the need to know.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 22 of 46

5. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

5.1 IDENTIFICATION OF UCNI

UCNI is certain unclassified government information concerning the design and security of nuclear facilities, materials, weapons, and components. It is controlled under section 148 of the AEA because its release would significantly increase the likelihood of the illegal production of a nuclear weapon or the theft, diversion, or sabotage of nuclear material, equipment or facilities.

UCNI includes the following categories:

- Production or utilization facility design information (includes design, operation, etc. of certain aspects of nuclear technologies, e.g., gas centrifuge, gaseous diffusion, etc.),
- Security measures for physical protection of production or utilization facilities or nuclear material contained in these facilities or in transit, and
- Declassified Restricted Data (e.g., nuclear weapon information).

Only an authorized UCNI RO with knowledge of the information being reviewed is authorized to make a determination that the document contains, or no longer contains UCNI. An UCNI RO authorizes the application of UCNI markings to or their removal from various documents. The UCNI RO's authority may not be delegated to anyone or exercised by a person acting for or in the absence of the RO.

5.1.1 Responsibilities of Originator or Possessor of Matter

5.1.1.1 Review Requirement

An UCNI RO determines whether the matter does or does not contain UCNI **based on guidance**. Any person who thinks unclassified documents or material he/she originates or possesses may contain UCNI must transmit this appropriately to an UCNI RO before it is finalized, sent outside of the organization or filed. The current list of UCNI ROs is provided on the Classification and Information Control Office home page. Also, the CICO staff (each member is an UCNI RO) is always available to answer any questions. The current list of CICO staff members is also provided on the Classification and Information Control Office home page.

5.1.1.2 Review Requirement Exceptions

The following matter is not required to be reviewed for UCNI:

- *Review exemption for documents in files.* Any document that was permanently filed prior to May 22, 1985, is not required to be reviewed for UCNI while in the files or when retrieved from the files for reference, inventory, or similar purposes as long as the document will be returned to the files and is not accessible by individuals who are not Authorized Individuals for the UCNI contained in the document. However, when a document that is likely to contain UCNI is removed from the files for dissemination within or outside of the immediate organization, it must be reviewed by an RO with cognizance over the information.
- Matter sent outside the originator's or possessor's organization for destruction. However, any matter being destroyed that is not marked as containing UCNI but that the originator or possessor believes may contain UCNI, must be destroyed in accordance with the CUI destruction procedures contained in this chapter.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 23 of 46

5.2 MARKING REQUIREMENTS FOR MEDIA CONTAINING UCNI

Appropriate markings shall be applied to any unclassified document or material that contains UCNI, regardless of any other unclassified control markings (e.g., Official Use Only, Proprietary) that are also on the document or material.

UCNI markings must not be applied to a classified document that contains UCNI, unless such document has been portion marked to indicate the classification level. In such cases, the acronym "UCNI" must be used to indicate those unclassified portions containing UCNI.

5.2.1 General UCNI Marking Requirements

Any unclassified document that has been reviewed and determined to contain UCNI information shall be marked on the front of the document or material as follows.

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

NOT FOR PUBLIC DISSEMINATION

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Reviewing Official: _____

(Name/Organization)

Date: _____

Guidance Used: _____

(List all UCNI guidance used)

The following marking (**UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION**) or (**UCNI**) shall be placed on the bottom of the front and back of the document and (1) on the bottom of each interior page of the matter, or (2) if more convenient, on the bottom of only those interior pages that actually contain UCNI (markings should be clearly visible).

See Attachment F for an example.

The originator is responsible for ensuring the title is reviewed by the UCNI RO. The title must indicate UCNI, if applicable. If the title provides another element of CUI (e.g., ECI or OUO), that designation must also appear before the title. Refer to Section 6.2 for further information when documents contain OUO and UCNI.

5.2.2 Marking Special Format Documents

Special formats of unclassified documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audio or videotapes, slides) must be marked to the extent practical as described above. Regardless of the precise markings used in such cases, any special-format, unclassified matter that contains UCNI must be marked so that both a person in physical possession of the matter (e.g., markings on a viewgraph frame, a film reel and its container) and a person with access to the information in or on the matter (e.g., markings on the projected image of a slide, a warning on a film leader) are made aware that it contains UCNI. When space is limited, as on a 35-mm slide, the "UCNI" marking will suffice.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 24 of 46

5.2.3 Transmittal Documents

A document that (1) transmits matter marked as containing UCNI, and (2) does not itself contain UCNI, must be marked on the front as follows:

Document(s) transmitted contain(s) Unclassified Controlled Nuclear Information. When separated from enclosures, this transmittal document does not contain UCNI.

See Attachment G for a visual example.

An UCNI document that (1) transmits matter marked as containing classified matter, and (2) does not itself contain classified information must be marked on the front as follows:

- Matter transmitted contains: Level and category of classified matter (e.g., Secret-Restricted Data, Confidential-National Security Information, etc.).
- When separated from enclosures, this transmittal document contains UCNI.

The UCNI transmittal document must meet all the UCNI marking and protection requirements contained in this manual.

5.2.4 Unclassified Matter That No Longer Contains UCNI

An UCNI RO or a Denying Official may determine that unclassified matter marked as containing UCNI no longer contains UCNI. In such a case, the official must ensure that all UCNI markings are removed or crossed out and that the front of the matter is marked as follows:

DOES NOT CONTAIN UNCLASSIFIED
CONTROLLED NUCLEAR INFORMATION
Reviewing/Denying Official: _____
(Name/Organization)
Date: _____

5.2.5 Unclassified Matter That Does Not Contain UCNI

An UCNI RO may determine that unclassified, unmarked matter does not contain UCNI. No markings are required in such a case; however, for documentation purposes, the UCNI RO may mark or may authorize the front of the matter to be marked with the same marking used in Section 5.2.5.

5.3 SECURING UCNI

Information generated by or for the Federal Government (Government Information) and identified by any UCOR/Subcontractor personnel as UCNI must be secured in accordance with the requirements of this manual.

5.3.1 Physical Media

Physical control shall be maintained over any physical media (paper documents, materials and equipment) marked as containing UCNI so as to prevent unauthorized access to the information.

Although not required, an UCNI cover sheet attached to the front of the document is a fast and cost effective method of meeting this requirement. The UCNI cover sheet is not a requirement, but considered a good business

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 25 of 46

practice. UCNI cover sheets do NOT take the place of any required markings to the document. UCNI cover sheets (Form-709) are available through UCOR Forms.

5.3.1.1 In Use

For an explanation of requirements, for routine or limited access to UCNI, see 10 CFR 1017.20 (routine access) or 10 CFR 1017.21 (limited access).

Each person granted access to UCNI must be notified of applicable regulations concerning UCNI prior to dissemination of the UCNI. Attaching an UCNI cover sheet (Form-709) to the front of the matter containing UCNI prior to its transmittal to the person constitutes notification.

An authorized individual, who may be the originator or possessor of UCNI, may grant routine access to UCNI to another Federal or contractor Government employees (refer to 10 CFR 1017 Subpart D for restrictions on requirements for non-US Citizens that are not employees) for such access simply by giving that person UCNI. No explicit designation or security clearance is required. The recipient of the UCNI becomes an Authorized Individual for that specific UCNI.

An authorized individual shall maintain physical control over any document, material or equipment in use that is identified as containing UCNI to prevent unauthorized disclosure.

Each person granted access to UCNI must be notified of applicable regulations concerning UCNI prior to dissemination of the UCNI. Attaching a UCNI cover sheet (Form-709) to the front of the matter containing UCNI prior to its transmittal to the person constitutes notification. In the area of UCNI awareness briefings, ensure that individuals with routine access to UCNI are briefed periodically in their responsibilities for identifying and protecting UCNI.

5.3.1.2 Reproduction

UCNI may be reproduced without permission of the originator. Reproduction shall be limited to the minimum number of copies necessary consistent with the need to carry out official duties. Reproduced copies shall be marked and protected in the same manner as the original document. Copy machine malfunctions must be cleared with all paper paths checked for UCNI material.

5.3.1.3 In Storage

Review exemption for documents in files. Any document that was permanently filed prior to May 22, 1985, is not required to be reviewed for UCNI while in the files or when retrieved from the files for reference, inventory, or similar purposes as long as the document will be returned to the files and is not accessible by individuals who are not Authorized Individuals for the UCNI contained in the document. However, when a document that is likely to contain UCNI is removed from the files for dissemination within or outside of the immediate organization, it must be reviewed by a Reviewing Official with cognizance over the information. Such matter may or may not have any UCNI markings.

When unattended, UCNI documents shall be stored in the following manner.

1. **On-Site.** In Limited Areas when UCNI documents, material or equipment are unattended, they may be stored with other unclassified matter in unlocked files, desks or similar containers. UCNI must not be left where unauthorized visual access is granted (e.g., left on a desk in an unlocked office, placed on a bulletin board in general use areas or GAAs or PPAs, or left unattended at a common printer or copier).

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 26 of 46

In the PPA or GAA, when UCNI documents, material or equipment are unattended, they shall be stored in a locked drawer, desk, file cabinet, or in a locked room.

2. **Off-Site.** In an area that is neither controlled nor guarded (i.e., a private residence or a subcontractor facility), UCNI documents, material or equipment shall be stored in a locked container or behind a locked door where physical control over the document is maintained. UCNI cannot be processed on a non-government approved computer.

5.3.1.4 Transmission

A document that (1) transmits an attachment or enclosure marked as containing an element of UCNI, and (2) does not itself contain an element of UCNI must be marked on the front or first page of the document as follows to call attention to the presence of UCNI in the attachment(s) or enclosure(s):



The designation that UCNI is being transmitted must appear on the first page of the transmittal document to ensure adequate protection is afforded to the controlled information. For example, a non-sensitive transmittal document transmitting UCNI would be marked UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION at the bottom of the transmittal and the statement “Document Transmitted Contains UCNI” appears at the bottom portion of the transmittal. See Attachment G for a visual example.

The designation that UCNI is being transmitted, by any of the means described below, is *not* annotated on the outside of the opaque envelope.

5.3.1.4.1 Within the ORR

Transmission shall be by means to preclude unauthorized disclosure or dissemination. A single, opaque envelope or wrapping must be used to transmit UCNI within the ORR. The opaque envelope or wrapping must be sealed and marked “TO BE OPENED BY ADDRESSEE ONLY.”

5.3.1.4.2 Outside the ORR

Transmission outside of the ORR is as follows.

1. A single, opaque envelope or wrapping must be used to transmit UCNI outside the ORR. The opaque envelope or wrapping must be sealed and marked, TO BE OPENED BY ADDRESSEE ONLY.
2. Any of the following U.S. mail methods may be used: U.S. First Class, Express, Certified, or Registered Mail.
3. Any commercial carrier using a signature service may be used.

5.3.1.4.3 Hand Carry Within or Outside the ORR

Authorized individuals (i.e., those who are granted access) shall hand-carry UCNI document between or within a facility as long as the authorized individual carrying the document can control access to the document being transported. The transporter must meet the access requirements and maintain constant control and vigilance over the UCNI matter. Visual access to the contents of the UCNI document shall not be permitted during transit.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 27 of 46

5.3.1.5 Destruction

A document marked as containing UCNI must be destroyed, at a minimum, by using a cross-cut shredder that produces particles no larger than ¼-inch wide and 2 inches long, or by any approved method for the destruction of classified matter.

5.3.2 Electronic Media

Physical control shall be maintained over any electronic media (electronic disks/chips/cards, videos) marked as containing UCNI so as to prevent unauthorized access to the information.

5.3.2.1 In Use and Reproduction

UCNI may be processed only on an AIS certified computer system with UCOR IT approval. AIS certified computer will have a US DOE government sticker or IT sticker on each piece of equipment. An AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to UCNI stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities. UCOR IT needs to know the file location of stored UCNI matter. UCNI may be reproduced without permission of the originator. Reproduction shall be limited to the minimum number of copies necessary consistent with the need to carry out official duties. Reproduced copies shall be marked and protected in the same manner as the original document. Copy machine malfunctions must be cleared with all paper paths checked for UCNI material.

5.3.2.2 In Storage

UCNI is protected in electronic form (e.g., computer files) when it resides on the approved AIS network and the file location has been approved by UCOR IT.

5.3.2.3 Transmission of Emails

UCNI may only be transmitted via UCOR email externally using Entrust.

5.3.2.3.1 Within the UCOR Firewall (name@ettp.doe.gov)

Ensure that email messages and attachments containing UCNI are marked as follows:

1. The first line of an email message containing UCNI must include the abbreviation “UCNI,” the Reviewing Official’s name and organization, and the guidance used to make the UCNI determination (e.g., UCNI; Jane Smith, HS-90; CG-SS-5). If there is an attachment that contains UCNI, it must have all required UCNI markings.
2. If the message itself is not UCNI but an attachment contains UCNI, the message must indicate that the attachment is UCNI. The attachment must have all required UCNI markings.

Examples of both an actual UCNI email and a non-sensitive email transmitting UCNI are shown in Attachment H and Attachment I, respectively.

5.3.2.3.2 Outside the UCOR Firewall

The email will be marked as noted in Section 5.3.2.3.1.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 28 of 46

UCNI (including protected PII) must be encrypted or password protected when emailed outside the UCOR firewall (email addresses other than name @ettp.doe.gov). Encryption can be accomplished by using one of the following methods: 1) Secure Email Gateway, 2) DOE Entrust Public Key Infrastructure, or 3) WinZip. Contact the UCOR Helpline (574-8000) for assistance with Secure Email Gateway (http://intranet.ettp.gov/IT/Help/pdf-docs/ETTP_MEG_Users.pdf), Entrust and WinZip.

If encryption is not available or some other form of protection is desired, the UCNI information may be included in a Microsoft office file or Adobe PDF file that is protected by a password and attached to the email message. Then, the sender sends the password in a separate email so that the recipient can access the file.

5.3.2.4 Transmission of Telecommunications

UCNI must be encrypted via an OMNI or secure telephone electronics. UCNI discussion must ensure the use of telecommunications services, including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities and radio communications, must consider and use the most secure means available for the transmission of UCNI over this form of media. These considerations include, but may not be limited to, physical, personnel, administrative, and communications protective features and any other supplemental controls established to provide an acceptable level of protection for UCNI. These protective features must deter access to UCNI by unauthorized individuals and restrict public releasability.

UCNI must be encrypted via an OMNI or secure telephone electronics when sending by facsimile. When sending UCNI by secure facsimile, the sender must contact the intended recipient to ensure an individual meeting the access requirements is ready to receive the transmission and that the fax is not left unattended. The sender is also responsible for making a follow-up phone call to the recipient to confirm that the entire UCNI document was received, that the UCNI is not left unattended on the fax machine, and that the faxed information is in the possession of authorized individual meeting the access requirements.

UCNI must not be transmitted over public switched broadcast communications paths (e.g., Internet).

5.3.2.5 Destruction

AIS media containing UCNI must be destroyed per instructions from UCOR IT Organization.

5.3.3 Human Beings

The transfer of knowledge including voice (telephonic, point-to-point), narrative message, presentations, radio and communications must consider and use the most secure means available for the transmission of UCNI over this form of media. These considerations include ensuring personnel without a need-to-know do not overhear voice communications in any form.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 29 of 46

6. DOCUMENTS CONTAINING OOU AND UCNI

6.1 IDENTIFICATION

Identification of OOU is discussed in Section 4.1 and identification of UCNI is discussed in Section 5.1.

6.2 MARKING REQUIREMENTS

MARKING OF FRONT PAGE – document is marked as an UCNI document with the addition of the OOU admonitory marking on the FRONT PAGE.

PAGE MARKING – the marking, “UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION” or “UCNI” must be placed on the bottom of the **front and back of the matter** and **for interior pages** may use only highest category of information (UCNI) in the document or on individual pages.

See Attachment J for a visual example.

6.3 SECURING

Secure the document using the highest category of information (UCNI) – refer to Section 5.3.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 30 of 46

7. TRAINING

7.1 MODULE 19938, CUI TRAINING

UCOR personnel and all UCOR subcontractors through sub-tier contractor personnel whose responsibilities include the generation, handling, use, storage, reproduction, transmission (including hand-carry), or destruction of CUI must successfully complete Training Module 19938, "CUI Training." The training must be completed every 12 months. Participants are encouraged to use the links provided when completing the test for this module. Participants must score a minimum of 80% on the examination provided at the end of the module. Documentation shall remain with each participant's training file for the renewal of this module, which is required every year. Individuals who need to complete Training Module 19938 and who do not have a UCOR computer account can contact the site Access Center to schedule training on a computer provided at the Access Center.

7.2 MODULE 031302, ETTP UCNI REVIEWING OFFICIAL TRAINING

UCOR personnel and UCOR subcontractors whose responsibilities include the generation or determination of UCNI documents must successfully complete Training Module 031302, "ETTP UCNI Reviewing Official Training." This initial training consists of a 6-hour classroom training and test.

Every two years, the UCNI RO must complete an ETTP UCNI refresher training course, which is usually computer-based training.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 31 of 46

8. CUI ASSESSMENT PROGRAM

CICO will perform impromptu and periodic assessments of UCOR/Subcontractor (1) personnel capabilities to identify and secure CUI, and (2) management understanding and implementing of CUI program requirements.

Assessments for UCNI will examine the following areas: UCNI authorities and UCNI guidance.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 32 of 46

9. CHANGES IN PERSONNEL STATUS

When an individual possessing CUI has their employment transferred or terminated, or upon the individual's death or non-duty status, the immediate supervisor must ensure that the following CUI issues are resolved:

- All CUI in the possession or custody of the person being transferred from or whose employment is being terminated with UCOR, UCOR subcontractor or sub-tier contractor are retrieved and transferred or reassigned.
- A Termination and Transfer Checklist (Form-123) for UCOR employees or a Subcontractor Staff Augmentation Employee Release Checklist (Form-655) for Subcontractor/sub-tier employees is completed. All required items listed on the form must be completed.
- No CUI is left unattended or abandoned.
- CUI, including "extra copies," is the property of the site contractor and/or subcontractor, and must not be removed from the contractor's control by any departing, including terminated, individual.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 33 of 46

10. IOSC AND INFRACTIONS

When there is a potential or actual compromise of CUI it must be immediately reported to Cyber Security. Cyber Security will then notify the IOSC IO as necessary. If an incident occurs outside of regular work hours, then notify the Park Shift Superintendent.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 34 of 46

11. RECORDS

All records shall be managed in accordance with PROC-OS-1001, *Records Management, Including Document Control*.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 35 of 46

Attachment A
DEFINITIONS/ACRONYMS
Page 1 of 3

Admonitory Markings – Warning notices specifying the authority and penalties associated with the elements of Unclassified Controlled Information.

AEA – Atomic Energy Act

AIS – Automated Information System

Applied Technology – Information related to engineering, development, design, construction, operation, or other activities pertaining to particular projects that are specified by the Office of Nuclear Energy on which a major funding emphasis has been placed or for which controlled distribution is required.

Authorized Individual – Any individual, employee or subcontractor who meets the need-to-know criterion and any other requirements for access to Unclassified Controlled Information.

CFR – Code of Federal Regulations

CI – Classified Information – Information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, as amended, or information determined to require protection against unauthorized disclosure under Executive Order 13526, as amended, or prior Executive orders, which is identified as National Security Information (NSI).

CICO – Classification and Information Control Office

CO – Classification Office

Compromise – Disclosure of Unclassified Controlled Information to unauthorized person(s). (See Unauthorized Disclosure.)

CUI - Controlled Unclassified Information – formerly Unclassified Controlled Information (UCI) – Data for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government interests. Some of the elements of CUI include Applied Technology, Cooperative Research and Development Agreement Information, OUO Information including ECI (OUO Ex. 3), PA Information, PI, and UCNI.

CUI* – CUI excluding UCNI and ECI (OUO, Exemption 3), but including OUO Exemptions 4, 5, 6, and 7.

DC – Derivative Classifier

DOE – U.S. Department of Energy

DOE-ORO – U.S. DOE-Oak Ridge Office

ECI – Export Controlled Information – Certain scientific and technical information products containing technical data, as defined in and controlled by the International Traffic in Arms Regulations, the Export Administration Regulations, the Nuclear Nonproliferation Act, and the Atomic Energy Act of 1954, as amended.

ETTP – East Tennessee Technology Park

FOIA – Freedom of Information Act

GAA – General Access Area

Information – Facts, data, or knowledge itself regardless of the medium of its conveyance. (Documents are deemed to convey or contain information and are not considered to be information per se.)

Infraction – The documentation issued through UCOR Security to individuals failing to comply with security requirements. The completed form is submitted to DOE.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 36 of 46

Attachment A
DEFINITIONS/ACRONYMS
Page 2 of 3

IO – Inquiry Official

IOSC – Incidents of Security Concern – 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.

IT – Information Technology

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

OMNI – A model of a secure telephone unit.

OPSEC – Operations Security – An unclassified term referring to a co-mingling of computer, technical counterintelligence security measures developed and implemented to augment traditional security programs (physical, information, personnel, and communications security) as a means of eliminating or minimizing vulnerabilities that impact on classified technical programs. This includes a continuing review of program operations so that information of net intelligence value is not inadvertently provided to an adversary or potential adversary.

Originator – The person who generates CUI in the form of a document (not the person who [only] prepared the master, determines the element of CUI, approves the issuance, or effects the reproduction).

ORNL – Oak Ridge National Laboratory

ORR – Oak Ridge Reservation

OUO – Official Use Only – A designation used by DOE to identify certain controlled unclassified information, which may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552).

PA – Privacy Act Information – Requires the protection of agency records maintained on individuals. The types of records which may be protected under the privacy act include: personnel and employment records, including PII; supervisor maintained personnel records; appraisal and development records; applications for employment; payroll and leave records; reports of financial interest; accounts payable and receivable; domestic travel records; foreign travel records; general training records; personnel medical records; employee assistance records; personnel exposure records; occupational and industrial accident records; equal opportunity complaint files; labor standards complaints and grievances; legal files; personnel security files; security investigations; employee and visitor access control records; and security education and infraction report records.

PI – Proprietary Information – Proprietary Information typically includes technical information, computer programs, financial information, strategic plans, marketing, customer, and vendor information, which is important to a corporation or company and is not publicly available.

PII – Personally Identifiable Information – Any information maintained by the DOE or its contractors about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual’s identity, such as his/her name, social security number, date and place of birth, mother’s maiden name, biometric data, etc., and including any other personal information that is linked or linkable to a specific individual.

PPA – Property Protection Area – A type of Security Area having boundaries identified with barriers and access controls for the protection of DOE property.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 37 of 46

Attachment A
DEFINITIONS/ACRONYMS
Page 3 of 3

PPII – protected PII

Public Release – Release to the public (accessible to any person) or such widespread external or internal distribution that release to the public is likely.

RO – Reviewing Official

Security Plan – An official document approved through the ETTP Site Contractor Security that describes the utilization of resources by a facility to provide protection of the facility, its site(s), and its assets from attack.

Sensitive Nuclear Technology – A category of nuclear information, the export of which from the U.S. is subject to certain conditions and controls specified in legislation, and is confined to information in the fields of uranium enrichment, nuclear fuel reprocessing, and heavy water production.

SGI – Sensitive Government Information

SME – Subject Matter Expert – An individual with expert knowledge and experience in a particular subject area.

STOI – Scientific, Technical/Technological and Operational Information related to a classified subject matter area

UCI – Unclassified Controlled Information (currently CUI)

UCNI – Unclassified Controlled Nuclear Information – Certain unclassified government information prohibited from unauthorized dissemination under Section 148 of the Atomic Energy Act of 1954, as amended. The protection control of UCNI is prescribed by 10 CFR 1017, and DOE O 471.1B.

Unattended Matter – Protected matter that is not in the direct custody or control of an individual meeting the access requirements.

Unclassified – (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 a Restricted Data, Formally Restricted Data, or National Security Information document, or a portion of an NSI document is not sensitive or controlled.

Y-12 – Y-12 National Security Complex

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 38 of 46

Attachment B
Example: OOU Document
Page 1 of 1

August 25, 20xx

UCOR-####Subject: Document Example

It is best if CUI documents have an unclassified nonsensitive title. If the title is OOU, then (OOU) will be placed before the title. If the title is UCNI, then (UCNI) will be placed before the title.

The OFFICIAL USE ONLY designation is only required at the bottom of the page; marking the top and bottom with OFFICIAL USE ONLY is acceptable. The first page must have the OFFICIAL USE ONLY designation and the OOU admonitory marking. The remaining pages can either (1) all be marked with OFFICIAL USE ONLY or, (2) after marking the first page of the document, only those pages actually containing OOU need to be marked. If marking the OOU document with option (2), the remaining pages following the front of the document that do not contain any CUI element can be left unmarked.

In the admonitory marking below, the correct Exemption Number and title of the Exemption must be included. The individual's name and organization who originated the OOU document must be completed in that portion of the admonitory marking, including the date.

As noted in Section 4.2.2, additional admonitory markings are required for Exemption 3 (refer to Section 4.2.2.1), Exemption 4 (refer to Section 4.2.2.2), and Exemption 6 (refer to Section 4.2.2.3). In addition to the general OOU markings, if a document contains a) ECI, b) Proprietary Information (PI), or c) Privacy Act (PA) Information, the bottom portion of the front page of the OOU document must be marked with an appropriate admonitory marking in addition to the general OOU markings (markings should be clearly visible). If a document has PII and ECI, then both admonitory markings must appear on the front page of the OOU document in addition to the general OOU markings.

<p>OFFICIAL USE ONLY</p> <p>May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), <u>Exemption Number 7, Law Enforcement</u></p> <p>Department of Energy review required before public release.</p> <p>Name/Org: <u>Jane Smith/ETTP CICO</u> Date: <u>01/XX/XX</u></p> <p>Guidance (if applicable) _____</p>
--

OFFICIAL USE ONLY

OOU markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 39 of 46

Attachment C
Example: Unclassified Hard Copy Memo Transmitting OOU
Page 1 of 1

To: Jane Doe
From: John Doe
Date: August xx, 20xx
Subject: Example of Memo

The element of CUI being transmitted must be indicated on the first page of the transmittal. On the lower portion of the transmittal, there must be a statement indicating that, when separated from the CUI, the transmittal is non-sensitive.

If the non-sensitive transmittal is a multi-page document, the succeeding pages of the transmittal need no markings since, standing alone, the transmittal contains no protected information.

Document transmitted
contains OFFICIAL USE ONLY

When separated from attachment,
this transmittal is NON-SENSITIVE

OFFICIAL USE ONLY

OOU markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 40 of 46

Attachment D
Example: Email Containing OOU
Page 1 of 1

From: Jane Doe
Sent: Tuesday, August XX, 20XX
To: John Doe
Subject: Marking of an Email Message

OOU. This is an example of an email message that contains Official Use Only. The first line of an email message containing OOU information must contain the abbreviation “**OOU**” before the beginning of the text.

If the email is forwarded, the **OOU** must be placed at the beginning of the forwarded email.

All email sent outside the UCOR firewall (recipients other than name@orcc.gov) must be encrypted or password protected. Encryption can be accomplished by using one of the following methods: 1) Secure Email Gateway, 2) DOE Entrust Public Key Infrastructure, or 3) WinZip. Contact the UCOR Helpline (574-8000) for assistance with Secure Email Gateway, Entrust and WinZip.

If encryption is not available or some other form of protection is desired, the OOU information may be included in a word processing file that is protected by a password and attached to the email message. Then, the sender can send the password in a separate email so that the recipient can access the file.

OOU or Official Use Only should not appear in the subject line of the email.

OOU markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 41 of 46

Attachment E
Example: Non-Sensitive Email Transmitting Official Use Only
Page 1 of 1

From: Jane Doe
Sent: Tuesday, August XX, 20XX
To: John Doe
Subject: Non-sensitive Email Example

Document Transmitted Contains OUO Information

An email that (1) transmits an attachment marked as containing OUO information and (2) does not itself contain classified or controlled information must be marked on the first line of the email to call attention to the presence of OUO information in the attachment.

The actual email text will begin after the above OUO caveat advising the recipient(s) that the attachment(s) contain OUO and must be protected and compliant with the PPD-SE-1415, *ETTP Controlled Unclassified Information Manual*, requirements.

If the email is forwarded, the “**Document Transmitted Contains OUO Information**” must be placed at the beginning of the forwarded email.

OUO or Official Use Only should not appear in the subject line of the email.

OUO markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 42 of 46

Attachment F
Example: UCNI Document
Page 1 of 1

August 25, 20xx

UCOR-####Subject: Document Example

Each document that contains UCNI must have the following markings:

The FRONT MARKING is placed on the front of each document that contains UCNI.

The name and organization of the Reviewing Official making the determination goes on the "Reviewing Official" line. The date the determination is made goes on the "Date" line. The short title of the guidance used to make the determination goes on the "Guidance Used" line. NOTE: To be consistent with the information contained on the "Derived From" line on a classified document, you may also add the approval date of the guidance and "DOE OC" after the short title of the guide. For example, then the "Guidance Used" line for an UCNI determination based on CG-SS-5 would read: "CG-SS-5, 7/22/2016, DOE OC." List all UCNI guidance used.

The PAGE MARKING is placed on the bottom of the front of each document and on the bottom of each interior page of the document that contains text or , if more convenient, on the bottom of only those interior pages that contain UCNI. These words must also be placed on the back of the last page of the document.

<p>UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).</p> <p>Reviewing Official: <u>John Smith/ETTP CICO</u> (Name/Organization)</p> <p>Date: <u>01/10/17</u> Guidance Used: <u>CG-SS-5, 7/22/16, DOE OC</u></p>
--

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

UCNI markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 43 of 46

Attachment G

**Example: Unclassified Hard Copy Memo Transmitting Unclassified Controlled Nuclear Information
Page 1 of 1**

To: Jane Doe
From: John Doe
Date: August xx, 20xx
Subject: Example Memo

A document that transmits documents or material marked as containing UCNI and does not itself contain classified information or UCNI must be marked on its front as follows:

Document(s) Transmitted contain(s)
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.
When separated from enclosures,
this transmittal document does not contain UCNI.

UCNI markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 44 of 46

Attachment H

Example: Non-Sensitive Email Containing Unclassified Controlled Nuclear Information Page 1 of 1

From: Jane Doe
Sent: Tuesday, August XX, 20XX
To: John Doe
Subject: UCNI Markings on Email Messages Example

UCNI; Paul Martinez, UP-32; CG-SS-5 – The first line of an email message must include the abbreviation “UCNI,” the Reviewing Official’s name and organization, and the guidance used to make the determination.

Reminder: An email message containing UCNI **must** be sent encrypted using Entrust when sent outside the UCOR firewall.

UCNI markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 45 of 46

Attachment I

Example: Non-Sensitive Email Transmitting Unclassified Controlled Nuclear Information Page 1 of 1

From: Jane Doe
Sent: Tuesday, August XX, 20XX
To: John Doe
Subject: Marking an Email Message with an UCNI Attachment Example
Attachments: Security Vulnerabilities at the ETTP Site

Document Transmitted Contains Unclassified Controlled Nuclear Information (UCNI)

The attachment to this message contains UCNI.

If the message itself is not UCNI but the attachment contains UCNI, the message must indicate that the attachment is UCNI, and the attachment must have all the required UCNI markings.

Reminder: An e-mail message with an UCNI attachment **must** be sent encrypted using Entrust when sent outside the UCOR firewall.

UCNI markings are for training purposes only.

OWNER: Security and Emergency Services	PPD-SE-1415
ETTP CONTROLLED UNCLASSIFIED INFORMATION MANUAL	REVISION: 4
	Page 46 of 46

Attachment J

Example: Document Containing both Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO)

Page 1 of 1

This is a sample of the front of a document that contains both UCNI and OUO information.

3. The front UCNI marking, which identifies the Reviewing Official with his or her organization, the date the UCNI determination was made, and the guidance used to make the determination, must be placed on front of the document. List all UCNI guidance used.
4. The words “Unclassified Controlled Nuclear Information” must be placed on the bottom of the first page.
5. The front OUO marking, which identifies the exemption number and category, name and organization of person making the determination, date of determination, and any guidance used, must also be placed on the front of the document.
6. Every interior page is marked at the highest level of information in the document (i.e., UCNI) or at the highest level of information on the page (i.e., either UCNI, OUO, or Unclassified).

<p>OFFICIAL USE ONLY</p> <p>May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), <u>Exemption Number 7, Law Enforcement</u></p> <p>Department of Energy review required before public release</p> <p>Name/Org: <u>John Smith/ETTP CICO</u> Date: <u>01/10/17</u> Guidance (if applicable) <u>CG-SS-5</u></p>

<p>UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION</p> <p>Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).</p> <p>Reviewing Official: <u>John Smith/ETTP CICO</u> (Name/Organization)</p> <p>Date: <u>01/10/17</u> Guidance Used: <u>CG-SS-5, 7/22/16, DOE OC</u></p>
--

OUO and UCNI markings are for training purposes only.

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION