UCOR
United Cleanup Oak Ridge LLC

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: 2/1/25 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
United Cleanup Oak Ridge LLC

OWNER: SSS – Integration – Safeguards, Security, and Emergency Services	**PPD-SE-1415**	**REVISION: 7**
SUBJECT MATTER AREA: Classification and Information Control	**PREPARER: Jacob Whitten**	**Page 1 of 50**
PROCESS/PROGRAM DESCRIPTION	**CONCURRENCE/DATE: Karl Klinger 1/22/24 [Approval Signature on File]**	
TITLE: UCOR CONTROLLED UNCLASSIFIED INFORMATION PROGRAM	**APPROVED BY/DATE: Leesa Laymance 1/9/24 [Approval Signature on File]**	
USQD ☐ UCD ☐ CAT X ☒ EXEMPT ☐	**EFFECTIVE DATE: 2/1/24**	
USQD/UCD/CAT X No: USQD-MS-CX-SECURITY-1733, Rev. 1	**REQUIRED REVIEW DATE: 2/1/25**	
Exhibit L Mandatory Contractor Document: No ☐ Yes ☒	**If an Interim Document, Expiration Date:**	

DOCUMENT IS UNCLASSIFIED, NON-SENSITIVE
APPROVED FOR PUBLIC RELEASE

Name/Organization: Dave Lannom/Classification
Date: 1/2/24
eIRO#: 40443

REVISION LOG

Revision	Effective Date	Description of Changes	Pages Affected
7	2/1/24	Intent change. Update the term "Protected" PII to "High Risk" PII per The Privacy Act. Update "STOI" to "STI" per DOE O 241.1B. Removed Form-260, East Tennessee Technology Park Document Release Form, since it is being retired and Form-368, UCOR Classification Review Request Form will be used exclusively.	6-12, 14-16, 23, 37, 39, 41
6	5/18/23	Intent change. Defined UCNI requirements and other equity reviews, Updated Section 4.3.2.3.1, Within the UCOR Firewall (name@orcc.doe.gov), and Section 4.3.2.3.2, Outside the UCOR Firewall. Corrected wording for Personal Privacy, Exemption 6.	All
5	10/24/22	Intent change Added eDC/RO e/IRO references to process steps detailed in PROC-SE-1005, R4, and newly revised UCOR-4388, *UCOR-CICO Review Policy for Newly Created-Media*. Change transmitting OUO instructions to current process approved by IT [must use Entrust for encryption when sending to DOE or password protected file]. Updated attachments with these new directions. On Page 3: Between 1. Introduction and 1.1 Program Definition, inserted a NOTE: The new DOE Order for CUI (DOE Order 471.7, issued February 3, 2022) […] Because UCOR's contract with DOE EM does not yet have DOE Order 471.7 in its contract, UCOR must still follow the requirements of the now-superseded Official Use Only Order and Manual. Updated 9.0 Change in Personnel Status – 2nd bullet. We only use one termination checklist now for both UCOR & Staff Aug.	3, 6-13,15, 16, 18, 20-22, 29, 30, 32, 34, 35, 37, 40-43, 46, 47
4	3/15/21	Non-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, *Bechtel Jacobs Company, LLC (BJC) Information Security (INFOSEC) Manual, Part II (*Rev. 6).	All

1. INTRODUCTION

NOTE:

Under Executive Order 13556, the entire Executive Branch of the U.S. Government must move to a new national standard regarding sensitive information called Controlled Unclassified Information (CUI). As implemented by the U.S. Department of Energy (DOE), the actual start dates for contractors (not federal employees) varies quite a bit. This variation in start dates is for the following reason:

The new DOE Order (O) for CUI (DOE O 471.7, issued February 3, 2022) states the following:

CANCELS/SUPERSEDES. DOE O 471.3 Chg. 1, *Identifying and Protecting Official Use Only Information*, dated 1-13-2011, and DOE Manual (M) 471.3-1 Chg. 1, *Manual for Identifying and Protecting Official Use Only Information*, dated 1-13-2011.

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

Because United Cleanup Oak Ridge LLC's (UCOR) contract with DOE Environmental Management (EM) does not yet have DOE O 471.7 in its contract, UCOR must still follow the requirements of the now-superseded Official Use Only (OUO) Order and Manual. In other words, UCOR continues to follow the familiar OUO requirements in this program description. The use of the term "controlled unclassified information" or CUI in this program description is therefore separate from the formal CUI program in DOE. It is a coincidence that UCOR and the U.S. Government use the same term.

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 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, 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 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 Security 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) 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 O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.3, *Administrative Change 1, Identifying and Protecting Official Use Only Information*
- DOE M 471.3-1, *Administrative Change 1, Manual for Identifying and Protecting Official Use Only Information*

1.2.2 Related UCOR Documents

- UCOR-4388, *UCOR-CICO Policy for Review of Newly Created Media*
- PROC-SE-1005, *Classification and Information Control*

2. RESPONSIBILITIES

2.1 UCOR SAFETY, SYSTEMS, AND SERVICES (SSS) – INTEGRATION – SAFEGUARDS MANAGER

The UCOR SSS – Integration – Safeguards 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 CUI is handled in accordance with the UCOR CUI Program requirements and CUI protection requirements are included in all UCOR protection program-planning documents.
- Approve any deviation from the requirements specified in this CUI program description.
- Ensure sufficient resources are provided for effective program execution.

2.2 PROJECT INTEGRATION AND BUSINESS SERVICES MANAGER

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

- Ensure 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** – controlled unclassified information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government interests. At UCOR, CUI includes 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 UCOR are:

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

UCNI is 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. UCNI is typically technical information associated with classified subject areas (CSA) (e.g., Gaseous Diffusion or Centrifuge, but not Security). See more detail in Sections 4 (OUO) and 5 (UCNI).

(2) **CUI*** means CUI excluding UCNI and ECI (OUO, Exemption 3), but including OUO Exemptions 4, 5, 6, and 7. **All staff have authority to determine information is CUI*. Consult CICO if needed.**

(3) **STI** means Scientific and Technical Information related to a classified subject matter area. All STI requires approval by the Classification Officer (CO) or his designee/CICO prior to its public release, unless CO has authorized its release via a written agreement with the information owner, which documents the information's non-sensitive status, i.e., a Designated Unclassified Subject Area (DUSA).

The UCOR CUI Program Manager is the UCOR CO. This individual reports to the UCOR Integration – Safeguards Manager and is responsible for the effective and efficient management of the UCOR CUI Program. Specific responsibilities include:

- Represent the UCOR Integration – Safeguards 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 former East Tennessee Technology Park (ETTP) CUI.
- Review, interpret, and comment on new or revised DOE orders and directives concerning potential CUI.
- Maintain company-level CUI programmatic procedures and guidance documents that provide for a consistent implementation of the UCOR 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.
- Review, comment, and approve UCOR 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 by CO (or CO-approved DC, i.e., CICO staff) guidance/approval required for Scientific and Technical Information related to a classified subject area (STI).

2.4 DERIVATIVE CLASSIFIERS (DCS)

DCs are responsible for making definitive OUO (Exemption 7, Law Enforcement) determinations by Classification Guidance and for providing expert advice to staff within their area of responsibilities/DC letter of authority.

Specific constraints/responsibilities include:

NOTE: If not ***absolutely certain*** that STI is not CUI/OUO, then protect and transfer information to CICO for definitive decision making.

- Definitive decision making that STI is **not** CUI/OUO by Classification Guidance.
- No public release of STI without CO or CICO guidance/approval (unless otherwise authorized by CO).
- Assure each individual within their area of responsibility understands the procedures for review of information that has the potential to contain CUI/OUO, can identify (potential) CUI/OUO, and understands the requirements for securing CUI/OUO (see Section 3.2.2).

2.4.1 DCs with Public Release Authority

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

2.5 UCNI Reviewing Officials (ROs)

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

Specific responsibilities include:

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

All definitive decisions that STI **is** UCNI must be confirmed by the CO or CICO.

- Definitive decision that STI is **not** UCNI.
- No public release of STI without CO/CICO guidance/approval (unless otherwise authorized by CICO).

- Assure 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 (see Section 3.2.2).

2.5.1 UCNI ROs with Public Release Authority

Some UCNI ROs (who are also DCs) have been granted public release of STI by the CO 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 media is released to the public by the CO or CICO.

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 STI does not contain CUI, then protect as CUI and obtain review through the Electronic Information Release Office system (eIRO).

- Definitive decision for CUI*; if not absolutely sure about CUI*, then check with a CUI* SME (e.g., CICO, UCOR Legal).
- No public release of STI without approval by CO or a CO-authorized individual (i.e., CICO staff).
- Follow all CUI requirements stated in this program description.
- Successfully complete Training Module 19938, Controlled Unclassified Information (CUI) Awareness Training, and any appropriate CUI training as determined necessary by CICO.
- Immediately report known or suspected incidents of compromise of CUI to Cyber Security.

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 UCOR and Subcontractor Termination Checklist (Form-123) for UCOR employees, Subcontractor Staff Augmentation, and Subcontractor/sub-tier employees is completed. All required items listed on the form must be completed.

- No CUI is left unattended or abandoned.

- Assure each person within their area of supervision can and does protect CUI according to this program description.

3. OVERVIEW OF CUI

3.1 PROTECTION OF CUI

The protection of CUI requires three activities: (a) identification of sensitive information or media requiring protection, (b) marking of the media, and (c) securing of media, which means controlling access to it. The term "media" is used to capture all entities that convey information. Examples of media are hardcopy documents, electronic files, such as emails, phone conversations, and the knowledge (i.e., information) held by an individual.

CUI media can be divided into three categories: (a) physical media, (b) electronic media, and (c) human beings. CUI must be protected as long as it exists. ***For hardcopy or electronic media***, this means protect it from its creation through its destruction. ***For human beings***, it means to control access to it using "need to know."

Once media is determined to no longer contain CUI, protection is no longer required, and any markings should be removed. For UCNI, this determination that media no longer contains UCNI 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 UCOR, there are two categories of CUI: OUO information and UCNI.

OUO Information is information that may be exempted from public release by FOIA. Types of OUO information relevant to UCOR are:

- Statutory Information (e.g., ECI) [Exemption 3],
- Commercial/Proprietary Information (PI) [Exemption 4],
- Privileged Information (e.g., DOE decision making information) [Exemption 5],
- Personal Privacy Information (PII)– including Privacy Act (PA) information [Exemption 6], and
- Law Enforcement Information (e.g., sensitive security-related and OPSEC information) [Exemption 7].

UCNI is 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.

Any developed UCNI guidance will be submitted by the UCOR CO to the Director, Office of Classification, for review and approval, in coordination with the Associate Administrator for Defense Nuclear Security for information under National Nuclear Safety Administration's (NNSA) cognizance prior to issuance, and will include: (1)the full text of the guidance; (2) a justification for any deviations from current policy proposed in the draft guidance; and (3) a point of contact for requesting copies of the guidance.

Once UCNI guidance is approved, within 30 calendar days UCOR CO will provide the Office of Classification with a file containing the approved guidance in either Microsoft Word or eXtensible Markup Language (XML). The UCOR CO ensures any UCNI guidance issued is revised when the guidance is no longer current or complete. At least once every five years, the UCOR CO will review all UCNI guidance to ensure it is up to date and will annotate the record copy of the guidance with the results of the review and the date it was performed. If the guidance is not current, it will be revised by the CO and submitted to the Director, Office of Classification, for approval, in coordination with the Associate Administrator for Defense Nuclear Security for information under NNSA's cognizance within 180 days of completing the review. Any new or revised UCNI guidance is distributed to appropriate UCNI ROs by the CICO manager within 30 calendar days to ensure they receive such guidance, and (1) destroy any superseded guidance or return it to the CO for destruction or (2) make page and/or pen-and-ink changes in guidance that has changed, as appropriate. The CO cancels the ROs authority when an individual no longer requires such authority or if an individual does not exercise the authority reliably. The CO or CICO manager will notify the individual and their supervisor of the reason for the cancellation and the effective date.

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 UCOR firewall***, that information must be reviewed for the presence of CUI (OUO and UCNI), or CUI*. If the information is potentially CUI* only, meaning it does not contain STI within a CSA, then **the originator should perform the review**, although it is strongly suggested if uncertainty exists then the information should be reviewed by a DC/CICO for final decision making.

DCs review for OUO and potential UCNI and UCNI ROs review for UCNI. If the DC/CICO determines there is information that is potentially UCNI, then a UCNI RO review must also be performed. Note UCOR DCs can also be UCNI ROs as documented on their authority letters, and if so, can review for both OUO and UCNI. The CO or CICO DCs can perform reviews for OUO, UCNI, and for public release, as documented on their authority letters.

If the information **contains STI within a CSA**, then CO or CICO review is **required prior to its public release unless** the CO has determined the information **exists within a DUSA**, and therefore, has authorized the release of the information publicly without review. If an originating person/group feels they routinely generate information within a CSA that could be deemed a DUSA by the CO, they should contact the CO or CICO and request approval.

Because UCOR manages work at **other sites** (i.e., Oak Ridge National Laboratory [ORNL] and Y-12 National Security Complex [Y-12]), STI related to a CSA or *equity* belonging to these sites must be reviewed by a CO/DC/RO certified by that site. Their review is sufficient for unlimited distribution if media is **site** generated and they authorize its public release for UCOR purposes. Normally, an Electronic Derivative Classifier/Reviewing Official system (eDCRO/RO) or eIRO form is generated by ORNL or Y-12 and is provided to UCOR to document their approval for public release of their equity. UCOR CO/CICO accepts this documentation as approval for public release of all equity. **No additional reviews required**.

If the **UCOR-generated media within a CSA is for public release** but **contains another sites equity**, then both (a) CO/CICO **and** (b) the ORNL and/or Y-12 Classification Offices (as appropriate) must perform the DC-UCNI RO reviews, and the Y-12 Information Release Office or the ORNL Technical Information Office (whichever is appropriate) must determine if their information is OUO. CICO can facilitate these reviews by either performing these (with agreement from the other sites) or by transferring media to the appropriate site reviewing entities.

All Staff:

- Ensure the review by the CO or CICO for any media—images, videos, reports, containing STI within a CSA (i.e., Isotope Enrichment, Nuclear Weapons, Safeguards and Security, etc.) prior to its public release.

  Refer to UCOR-4388, *UCOR-CICO Policy for Review of Newly Created-Media*, for more information.

  Refer to the *UCOR CSA Staff Briefing* and the CICO website for a list of **current UCOR CSAs**.

  Check for applicable **DUSAs**.

  Use the preferred method of the **unclassified eIRO review system** to obtain approval from CICO Staff.

  Use the ***Alternate Routing*** option in **eIRO** in conjunction with Form-368, United Cleanup Oak Ridge LLC (UCOR) Review Request Form, for legacy ETTP media **and** for newly created media that cannot be uploaded to the unclassified system for any reason.

  When in doubt, contact your CO or CICO Staff for definitive decision making prior to uploading media to eIRO or distributing STI or any information within a CSA outside of the UCOR firewall.

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. It is important that media containing CUI be marked properly; checking with CICO is recommended.

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 in the performance of official 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 program description 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 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 for a definitive decision making**. 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 UCOR controls), and (e) Destruction. Each activity has associated protocols. 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 these tools could back up information to the cloud, which is, essentially, setting them up for public release of UCOR information. When you use your personal devices to create site data, ensure you are protecting that information in accordance with all UCOR procedures; this includes sending it securely over UCOR-approved email, deleting it and/or removing it from your device when no longer needed. Data can take many forms, such as voice recordings, photos, videos, emails, and notes. It is your responsibility to handle and protect all UCOR information, no matter what form it takes or how it was created.

Decision Making Assistance. DCs in your organization and CO/CICO staff are useful resources for questions about CUI. The current list of DCs is provided on the Classification & Information Control Office home page. The current list of CICO Staff is also provided on the Classification & Information Control Office home page. It is important to note STI that may be OUO or ECI must be secured and transferred to CICO for definitive decision making. Upload to eIRO for review.

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 government 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 Classification Guidance applies, or (b) both of the criteria in 1) and 2) above are met. The CO has definitive decision-making authority for both*.

With the exception of sensitive safeguards and security information (OUO, Exemption 7) as determined by Classification Guidance CG-SS-5, there is little specific written guidance to assist in OUO decision making. In general, personnel who are uncertain whether or not media contains CUI (OUO or UCNI) or CUI* (Exemption 4, 5, 6, 7-not by Guidance) should consult their DC, CO, or CICO staff for assistance or a definitive determination.

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 CUI (OUO and UCNI) information still contains CUI information. Until that determination is made, the media marked as CUI must continue to be handled securely. Information that is determined OUO by Classification Guidance remains OUO until Classification Guidance indicates it is no longer OUO. A DC, CO, or CICO makes the final determination.

4.1.3 OUO FOIA Exemptions

Circumvention of Statute, Exemption 2

Prior to June 1, 2011, sensitive security information was marked as OUO Exemption 2. Policy 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 five 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).
- 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 UCOR is ECI. ECI is a category of information DOE established as a nonproliferation tool. It is defined as unclassified technical information by which distribution is subject to export control and which unrestricted public dissemination could provide significant assistance to proliferants or potential adversaries of the United States.

ECI at UCOR including the former ETTP site 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 U.S. Department of 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 STI that has the potential to be ECI (meaning STI related to a CSA) ***must be referred to CICO for definitive decision making*** *via eIRO.*

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 OUO 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.

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 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 OUO under Exemption 5:

1. The information must be for inter-agency or intra-agency communication only. This means 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

Personally Identifiable information (PII) is personal information associated with a specific individual (or individuals). High Risk Personally Identifiable information is information that, if disclosed, could reasonably be expected to cause damage to the individuals concerned (e.g., personal distress or embarrassment or could lead to identify theft).

Examples of High Risk PII include PII for which the government has responsibility to collect and protect:

- 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 High Risk PII.

Privacy Act (PA) information includes PII protected by the Privacy Act. PA information is protected as OUO Exemption 6; and there are specific requirements in addition to Exemption 6 as defined by DOE O 206.1.

Law Enforcement, Exemption 7

At UCOR, 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 Classification Guidance CG-SS-5 or as an OPSEC concern based on local security expertise.

Examples of security-related OUO which is based on topical classification 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 or Guidance:

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, and 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.

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.

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 USC 552), exemption number and category: _____

_____

Department of Energy review required prior to public release.

Name/Org: _____ Date: _____

Guidance, if applicable: _____

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). If space is limited, "OUO" may be used instead. 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 OUO requirements to recipients. The Official Use Only (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 document in addition to 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

4.2.2.2 Proprietary Information (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 Privacy Act (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 classification guidance may be removed by any personnel when the classification guidance used to make the determination states the information is no longer OUO. (For example, a topic may state 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.). Check with your DC/CO/CICO for definitive determination prior to removing.

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 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) DC/CO/CICO.

Markings Applied Based on Guidance or Criteria Stated in Section 4.1.1: After it has been confirmed that no OUO exists in the document, then a) the general OUO 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:

DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION

Name/Org. Date:

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 DC (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 OUO

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

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 OUO 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 OUO 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 for UCOR business purposes.

4.3.1.2 Reproduction

OUO 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 OUO material. Care must be taken that the contents cannot be viewed during reproduction by an individual without an appropriate need to know.

4.3.1.3 In Storage

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

1. **Onsite.** In the Limited Area, when OUO documents, material, or equipment are unattended, they may be stored with other unclassified matter in unlocked files, desks, or similar containers. OUO 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 OUO documents, material, or equipment are unattended, they shall be stored in a locked drawer, desk, file cabinet, or in a locked room.

2. **Offsite.** In an area that is neither controlled nor guarded (i.e., a private residence or a subcontractor facility), OUO documents, material, or equipment shall be stored in a locked container or behind a locked door where physical control over the document is maintained. OUO 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 OUO, and (2) does not itself contain OUO must be marked on the front or first page of the document as follows to call attention to the presence of OUO in the attachment(s) or enclosure(s):

Document(s) Transmitted
Contain(s) OUO Information

The type of OUO (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 OUO would be marked **OFFICIAL USE ONLY** at the very bottom of the transmittal document and the statement "Document Transmitted Contains OUO" appears at the bottom portion of the transmittal. See Attachment C for an example.

The specific type of OUO being transmitted by any of the means described below, is ***not*** annotated on the outside of the opaque envelope. OUO 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 OUO 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 OUO 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.

4.3.1.4.3 Hand Carry Within or Outside the ORR

Authorized individuals (i.e., those who are granted access) shall hand-carry OUO 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 OUO matter. Visual access to the contents of the OUO document shall not be permitted during transit.

4.3.1.5 Destruction

Any document or material identified as containing OUO 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 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 OUO from the site must either return it to the site for proper storage and/or destruction or provide the OUO to an appropriately trained individual (with need to know) who knows how to handle, store, and destroy OUO.

4.3.2 Electronic Media

Physical control shall be maintained over any electronic media marked as containing OUO to prevent unauthorized access to the information.

4.3.2.1 In Use and Reproduction

OUO 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 OUO 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 OUO files that reside on the UCOR system. Personnel are not allowed to save any OUO files to their home computer or any other electronic device unless approved by UCOR IT.

4.3.2.2 In Storage

OUO 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 OUO 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.

4.3.2.3 Transmission of OUO By Email

Emails containing OUO information (as listed in Section 4.1.3) must contain the acronym OUO before the text in the first line of the message—**not in the email subject line**.

If an email attachment contains OUO, the first line of the message should read, **Document Transmitted Contains OUO Information.** OUO or Official Use Only should not appear in the subject line of the email. The OUO attachment must be appropriately marked as OUO as described in Section 4.2.1.

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

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

The email must be marked as noted in Section 4.3.2.3.

No encryption or password protection is required when transmitting OUO, including PII, within the UCOR Firewall.

Contact the UCOR Helpline (865-574-8000) or UCOR Cybersecurity (cybersecurity@orcc.doe.gov) for questions concerning sending OUO, including PII, from within the UCOR Firewall.

4.3.2.3.2 Outside the UCOR Firewall

The email must be marked as noted in Section 4.3.2.3.

Emails to DOE, DOE contractors, and others (anyone who does not have a "@orcc.doe.gov" email address) that contain OUO information, must be encrypted or password protected.

1. Outside the UCOR Firewall to DOE or DOE contractors and laboratories – Entrust encryption preferred but password protection is allowed (Microsoft O365 encryption is not allowed).

2. Outside the UCOR Firewall to anyone other than DOE or DOE contractors and laboratories – Encryption is required and can be completed via Entrust, Microsoft O365 encryption (i.e., place "[secure]" or "[encrypt]" in the subject line of the email before the subject text), or password protect the OUO.

3. An OUO subset, PII, or High Risk PII, must be marked as "Official Use Only" and preferably encrypted when sending to anyone. Alternatively, a password protected file can be used.

4. With a password protected attachment, the password must be sent to the recipient in a separate email, or one can call the recipient to give the password.

DO NOT assume it is okay to send OUO information non-secure due to recipient(s) not having Entrust, or due to expediency of a request to provide this information to external recipients.

NOTE: **With Entrust, the receiving party must also have a valid Entrust certificate to receive and read the email**. Alternatively, call the recipient(s) and ask how the OUO information should be sent, and if a password-protected file would suffice.

If you do not already have an Entrust account setup, or have forgotten your Entrust password, please submit a trouble ticket at helpline@orcc.doe.gov or submit a Service Request Ticket at https://sdp.ettp.gov.

- See How to Send/Receive Encrypted Emails.
- Contact the UCOR Helpline (865-574-8000) or Cybersecurity Team (cybersecurity@orcc.doe.gov) for encryption assistance.
- Contact DC/CO/CICO staff for OUO guidance.

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.

Transmission of unencrypted/unprotected PII outside of the UCOR Firewalls must be reported to cybersecurity within 45 minutes of discovery.

4.3.2.4 Transmission by Telecommunications

The information sender must consider and use the most secure means available for the transmission of OUO through telecommunications, including voice circuits and facsimile, to protect access to the OUO information by unauthorized individuals and restrict its 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 the fax is not left unattended. The sender is also responsible for making a follow-up phone call to the recipient to confirm the entire OUO document was received, the OUO is not left unattended on the fax machine, and the faxed information is in the possession of authorized individual meeting the access requirements.

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 CUI (OUO and UCNI) or CUI* must be destroyed per instructions from UCOR IT.

4.3.3 Human Beings

Knowledge that contains CUI or 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 cannot protect it appropriately.

Information is defined as facts, data, or knowledge itself regardless of the medium of its conveyance. The transfer of information including voice communications, emails, presentations, etc., requires consideration and use of the most secure means available. Considerations include ensuring personnel without a need to know do not overhear voice communications, transmitting emails securely, and assuring before presentations/discussions that participants have the need to know.

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 is 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).

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. CICO must confirm all UCNI determinations.

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 front of documents sent outside of an originator's or possessor's organization for UCNI review must be marked with ''Protect as UCNI Pending Review.". The current list of UCNI ROs is provided on the Classification & Information Control Office home page. Also, the CICO staff (each member is a UCNI RO) is always available to answer any questions and confirm any determination of UCNI by an UCNI RO. The current list of CICO staff is also provided on the Classification & Information Control 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.

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., OUO) 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**) if space is limited, 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 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.

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 program description.

5.2.4 Unclassified Matter That No Longer Contains UCNI

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

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

An UCNI RO or a Denying Official also ensures unclassified documents from which UCNI has been redacted are marked to clearly indicate it is a redacted version.

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 5.2.4.

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 program description.

5.3.1 Physical Media

Physical control shall be maintained over any physical media (paper documents, materials, and equipment) marked as containing UCNI 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 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 1017.20(b)(1)(i)-(viii) for other U.S. citizens allowed access for government purposes and 10 CFR 1017 Subpart D for restrictions on requirements for non-U.S. Citizens that are not employees) to perform official duties or DOE-authorized activities (i.e., has a need to know). 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 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 RO 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. **Onsite.** 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).

   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. **Offsite.** 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

The first line of an email message containing UCNI must include the abbreviation "UCNI," the RO's name and organization, and the guidance used to make the determination, before any email text.

An email or document that (1) transmits an attachment or enclosure marked as containing UCNI, and (2) does not itself contain 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):

Document Transmitted
Contains UCNI

The designation that UCNI is being transmitted must appear on the front or 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.

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 to prevent unauthorized access to the information.

5.3.2.1 In Use and Reproduction

NOTE: Currently, UCOR does not have an AIS file location documented as approved for the storage of UCNI. If one is needed, contact UCOR IT and CICO.

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

NOTE: Currently, UCOR does not have an AIS file location documented as approved for the storage of UCNI. If one is needed, contact UCOR IT and CICO.

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

NOTE: Currently, UCOR does not have an AIS (e.g., computer system) approved for the storage and transmission of UCNI. If one is needed, contact UCOR IT and CICO.

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

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

Ensure 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 markings.

2. If the message itself is not UCNI but an attachment contains UCNI, the message must indicate 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

NOTE: Currently, UCOR does not have an AIS approved for the storage of UCNI. If one is needed, contact UCOR IT and CICO.

The email will be marked as noted in Section 5.3.2.3.1.

UCNI must be encrypted when emailed outside the UCOR firewall (email addresses other than name @orcc.doe.gov). Encryption can be accomplished by using the following method: DOE Entrust Public Key Infrastructure.

5.3.2.4 Transmission of Telecommunications

NOTE: Currently, UCOR does not have an AIS approved for the storage of UCNI, and does not have an OMNI or secure telephone electronics. If one is needed, contact UCOR IT and CICO.

UCNI must be transmitted via an OMNI or secure telephone electronics.

UCNI must be transmitted 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 the fax is not left unattended. The sender is also responsible for making a follow-up phone call to the recipient to confirm the entire UCNI document was received, the UCNI is not left unattended on the fax machine, and 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 and CICO.

5.3.3 Human Beings

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

6. DOCUMENTS CONTAINING OUO AND UCNI

6.1 IDENTIFICATION

Identification of OUO 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 OUO admonitory marking on the FRONT PAGE.

PAGE MARKING – The marking, "UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UCNI" if space is limited, must be placed on the bottom of the **front and back of the matter** or front page and back of the last page of a document, and **for interior pages**, one may use the highest category of information in the document, for instance UCNI, on all pages or mark individual pages with the highest category of information on that page.

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.

7. TRAINING

7.1 MODULE 19938, CONTROLLED UNCLASSIFIED INFORMATION (CUI) AWARENESS TRAINING

UCOR personnel and all UCOR subcontract augmentation or subcontractor/sub-tier personnel whose responsibilities include the generation, handling, use, storage, reproduction, transmission (including hand-carry), or destruction of CUI and CUI* must successfully complete Training Module 19938, Controlled Unclassified Information (CUI) Awareness Training, as assigned by CICO. 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. Documentation shall remain within each participant's training file. 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 their computer training. Currently, only personnel designated as "Craft" are exempt from the CUI Training.

7.2 MODULE 031302, ETTP UCNI REVIEWING OFFICIAL TRAINING

UCOR personnel and UCOR subcontract augmentation or subcontractor/sub-tier personnel 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 six hour classroom training and test.

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

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.

9. CHANGES IN PERSONNEL STATUS

When an individual possessing CUI or CUI* has their employment transferred or terminated, or upon the individual's death or non-duty status, the immediate supervisor must ensure the following 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 UCOR and Subcontractor Termination Checklist (Form-123) for UCOR employees or subcontractor augmentation or subcontractor/sub-tier personnel is completed. All required items listed on the form must be completed.
- No CUI is left unattended or abandoned.
- All 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.

10. INCIDENTS OF SECURITY CONCERN (IOSC) AND INFRACTIONS

When there is a potential or actual compromise of CUI and CUI*, including High Risk PII, it must be immediately reported to Cyber Security. PII incidents must be reported within 45 minutes of discovery.

11. RECORDS

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

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 criteria and government business-related requirements for access to Controlled Unclassified 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 Officer

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

CSA – classified subject areas

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. Elements of CUI include OUO Information including ECI (OUO Ex. 3) and UCNI.

CUI* – CUI excluding ECI (OUO, Exemption 3) and UCNI, but including OUO Exemptions 4, 5, 6, and Exemption 7 – not determined by classification guidance.

DC – Derivative Classifier

DOE – U.S. Department of Energy

DUSA – Designated Unclassified Subject Area

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.

eIRO – Electronic Information Release Office system

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.)

Attachment A
Definitions/Acronyms
Page 2 of 3

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

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 Organization

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.

NNSA – National Nuclear Safety Administration

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 classified technical programs. This includes a continuing review of program operations so 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 Personally Identifiable information (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.

Attachment A
Definitions/Acronyms
Page 3 of 3

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

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 Emergency Services Watch Office 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.

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

SSS – Safety, Systems, and Services

STI – Scientific and Technical Information related to a classified subject area.

UCI – Unclassified Controlled Information (currently CUI)

UCOR – United Cleanup Oak Ridge LLC

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 media (information, 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 a declassified document, page, or title of a Restricted Data, Formally Restricted Data, or National Security Information (NSI) document, or a portion of an NSI document is not sensitive or controlled.

Y-12 – Y-12 National Security Complex

Attachment B
Example: OUO Document
Page 1 of 1

August 25, 20xx

UCOR-####Subject: Document Example

It is best if Controlled Unclassified Information (CUI) documents have an unclassified nonsensitive title. If the title is OUO, then (OUO) 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. The first page must have the OFFICIAL USE ONLY designation and the OUO 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 OUO need to be marked. If marking the OUO document with option (2), the remaining pages following the front of the document that do not contain any OUO 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 OUO 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 OUO 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 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 Personally Identifiable Information (PII) and Export Controlled Information (ECI), then both admonitory markings must appear on the front page of the OUO document in addition to the general OUO markings.

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category:
Exemption Number 7, Law Enforcement

EXAMPLE

Department of Energy review required before public release.

Name/Org: Jane Smith/UCOR CICO Date: 01/XX/XX
Guidance (if applicable) CG-SS-5, 7/22/2016, DOE OC

OFFICIAL USE ONLY

OUO markings are for training purposes only.

Attachment C
Example: Hard Copy Memo Transmitting OUO
Page 1 of 1

To: Jane Doe

From: John Doe

Date: August xx, 20xx

Subject: **Example of Memo**

The element of Controlled Unclassified Information (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, 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

OUO markings are for training purposes only.

Attachment D
Example: Email Containing OUO
Page 1 of 1

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

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

OUO or Official Use Only should not appear in the subject line of the email. Email sent outside the UCOR firewall (recipients other than name@orcc.doe.gov) must be encrypted or password protected.

1. Outside the UCOR Firewall to DOE or DOE contractors and laboratories – Entrust encryption preferred but password protection is allowed (Microsoft O365 encryption is not allowed).

2. Outside the UCOR Firewall to anyone other than DOE or DOE contractors and laboratories – Encryption is required and can be completed via Entrust, Microsoft O365 encryption (i.e., place "[secure]" or "[encrypt]" in the subject line of the email before the subject text), or password protection of the OUO attachment is allowed. The OUO attachment must be marked as "Official Use Only."

3. An OUO subset, PII that is considered High Risk Personally Identifiable Information, must be marked as "Official Use Only" and preferably encrypted when sending to anyone. Alternatively, a password protected file can be used.

4. With a password protected attachment, the password must be sent to the recipient in a separate email, or one can call the recipient to give the password.

Contact the UCOR Helpline (865-574-8000) for assistance with encryption. See How to Send/Receive Encrypted Emails.

If encryption is not available, the OUO information may be included in a word processing file or PDF, etc., that is protected by a password and attached to the email. Then, the sender sends the password in a separate email to the recipient or calls the recipient with the password so they can open the file.

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

OUO markings are for training purposes only.

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 Official Use Only (OUO) information and (2) does not itself contain OUO must be marked on the first line of the email to call attention to the OUO attachment.

The actual email text will begin after the OUO caveat "**Document Transmitted Contains OUO Information.**"

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

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

OUO markings are for training purposes only.

Attachment F
Example: UCNI Document
Page 1 of 1

August 25, 20xx

UCOR-####Subject: Document Example

Each document that contains Unclassified Controlled Nuclear Information (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.

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: John Smith/UCOR CICO
(Name/Organization)
Date: 01/10/17
Guidance Used: CG-SS-5, 7/22/16, DOE OC

EXAMPLE

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

UCNI markings are for training purposes only.

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 Unclassified Controlled Nuclear Information (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.

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.

UCNI markings are for training purposes only.

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 the attachment is UCNI, and the attachment must have all the required UCNI markings.

Reminder: An email message with an UCNI attachment **must be sent encrypted using Entrust.**

UCNI markings are for training purposes only.

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.

1. 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.

2. The words "Unclassified Controlled Nuclear Information" must be placed on the bottom of the first page.

3. 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.

4. 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).

OFFICIAL USE ONLY
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: Exemption Number 7, Law Enforcement

Department of Energy review required before public release

Name/Org: John Smith/UCOR CICO Date: 01/10/17
Guidance (if applicable) CG-SS-5

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: John Smith/UCOR CICO
(Name/Organization)

Date: 01/10/17
Guidance Used: CG-SS-5, 7/22/16, DOE OC

EXAMPLE

OUO and UCNI markings are for training purposes only.

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION