U.S. Department of Energy
Washington, DC

ORDER

DOE O 471.7

Approved: 2-3-2022

SUBJECT: CONTROLLED UNCLASSIFIED INFORMATION

1. PURPOSE. Establish the Department of Energy's (DOE) Controlled Unclassified Information (CUI) Program and document a policy for designating and handling information that qualifies as CUI. The CUI Program standardizes the way DOE handles information that requires protection under laws, regulations, or Government-wide policies (LRGWP), but that does not qualify as classified under Executive Order (EO) 13526, Classified National Security Information, 12-29-2009 (3 Code of Federal Regulations (CFR), 2010 Comp., p. 298-327), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq.), as amended. This Directive implements the requirements in EO 13556, Controlled Unclassified Information, and 32 CFR part 2002, Controlled Unclassified Information.

2. CANCELS/SUPERSEDES. DOE Order (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contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. This directive applies to all Departmental Elements.

      (1) The Administrator of the National Nuclear Security Administration (NNSA) must ensure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

      (2) The Administrator of Bonneville Power Administration must ensure that its employees and contractors comply with their respective responsibilities under this directive.

   b. DOE Contractors. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Order that apply to certain Management and Operating (M&O) contracts and non-M&O Major Site/Facility contracts as determined by the Heads of Departmental Elements (HDEs).

c. Equivalencies/Exemptions for DOE O 471.7.

(1) A request for an exemption from this Directive or an equivalency determination over all or some of the Element's CUI marking, safeguarding, and destruction requirements while the CUI remains within DOE control should be submitted for approval to the Departmental Element Designated CUI Official. Reports of approved equivalencies and exemptions must be sent to the Senior Agency Official (SAO) for CUI to maintain visibility over the equivalencies and exemptions. Such requests must:

(a) Identify the requirement for which an equivalency or exemption is being requested;

(b) The rationale as to why the equivalency or exemption is needed; and

(c) The alternate steps to be taken to ensure sufficient protection.

(2) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS.

a. Identifying Controlled Unclassified Information (CUI). CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a LRGWP requires or permits an agency to handle using safeguarding or dissemination controls.

(1) CUI categories approved by National Archives and Records Administration (NARA), the CUI Executive Agent (EA), published in the CUI Registry, and authorized for DOE use, are the exclusive designations for identifying CUI within DOE.

(2) No other safeguarding and dissemination controls can be implemented for any controlled unclassified information other than those permitted by the applicable LRGWP and as indicated in the CUI Registry. The CUI Registry can be found at https://www.archives.gov/cui.

(3) DOE personnel who have a Lawful Government Purpose (LGP) can be authorized holders and identify information as CUI, according to 32 CFR part 2002.30 (refer to Section 2002.4(bb) definition of Lawful Government Purpose), unless the applicable LRGWP imposes additional

requirements. However, authorized holders may only handle CUI when furthering a LGP. At DOE, an authorized holder's LGP may be defined by DOE policy, position descriptions, or contractual requirements.

(4) For information to be identified as CUI, it must be designated as either of the two types of CUI: CUI Basic or CUI Specified.

(a) CUI Basic is the subset of CUI for which the authorizing LRGWP does not set out specific safeguarding or dissemination controls. CUI Basic is handled according to the uniform set of controls in 32 CFR part 2002, this Directive, and the CUI Registry. If safeguarding and dissemination controls are not contained in the LRGWP, CUI Basic controls apply.

(b) CUI Specified is the subset of CUI in which the authorizing LRGWP contains specific handling controls that it requires or permits agencies to use, and which differ from those controls for CUI Basic. Safeguarding and dissemination controls contained in LRGWP take precedence over the requirements in 32 CFR part 2002. CUI Basic controls apply whenever CUI Specified controls do not cover the involved CUI.

(5) If new Categories of CUI are needed, the Departmental Element's Designated CUI Official must submit a request for consideration to the DOE SAO for CUI, who will then submit the request to NARA. The request must contain the following information, as applicable:

(a) The information type that requires protection;

(b) The commitment to sponsor or issue a LRGWP or a citation to an existing LRGWP;

(c) The anticipated date or timeframe for the release of the proposed LRGWP related to the information; and

(d) Any supporting authorities that help establish the need or justification for the proposed LRGWP, any drafts of the proposed authority DOE plans to develop, information on any development steps already undertaken and where DOE is in the development process for the proposed authority, and any other relevant information.

b. CUI Specified. This section identifies CUI Specified commonly used within DOE. Additional categories of CUI Specified are identified in the CUI Registry and in DOE program guidance.

(1) Unclassified Controlled Nuclear Information (UCNI). Requirements for the identification and protection of UCNI are contained in section 148 of

the Atomic Energy Act, Title 10 CFR, part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*; and DOE O 471.1, *Identification and Protection of Unclassified Controlled Nuclear Information*, current version.

(2) Privacy Information. Requirements for the marking and safeguarding of personally identifiable information (PII) under CUI are outlined in DOE O 206.1, *Department of Energy Privacy Program*, current version. PII must be handled in accordance to the level of sensitivity, with more sensitive categories, i.e., Social Security Numbers, financial records, and medical records, being safeguarded through encryption or password-protection. Privacy information, in either physical or electronic format, which is collected, used, processed, maintained, stored, shared, or transferred within DOE should be marked and safeguarded under the requirements of this Directive and 32 CFR part 2002. CUI Specified markings may be applicable under the Privacy Act of 1974 (Title 5 U.S. C. 522a) or Office of Management and Budget directives.

(3) Export Controlled Information. Information (which may include technology, technical data, assistance or software), the export (including, as applicable, transfer to foreign nationals within the United States) of which is controlled under the "Export Administration Regulations" (maintained by the U.S. Department of Commerce), the "International Traffic in Arms Regulations" (maintained by the U.S. Department of State), "10 CFR Part 810, Assistance to Foreign Atomic Energy Activities" regulations (maintained by the U.S. Department of Energy), or various trade and economic sanctions (maintained by the U.S. Department of Treasury's Office of Foreign Assets Control).

(4) Unclassified Naval Nuclear Propulsion Information (U-NNPI). U-NNPI is unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

c. Access and Sharing.

(1) Access to CUI is restricted in accordance with applicable LRGWP that requires it.

(2) CUI may only be disseminated and shared with persons in accordance with an LGP and who are eligible for access under applicable LRGWP.

(3) CUI must not be released through unapproved methods (e.g., posted on a publicly accessible website). All procedures for public release of CUI, except for those under the Privacy Act, the Freedom of Information Act

(FOIA), and Mandatory Declassification Reviews (MDR) procedures, of CUI must be approved by the Departmental Element Designated CUI Official.

(4) When transmitting CUI by mail, it can be shipped through interagency mail systems, United States Postal Service (USPS), or other commercial delivery services, consistent with other provisions of law. In-transit automated tracking and accountability tools can be used to record the location of the CUI Specified. Furthermore, while CUI documents and matter being mailed must be properly labeled, the wrapping or package containing the CUI must not indicate the presence of CUI. The wrapping or package should indicate "Open by Addressee Only" to ensure it is only opened by the intended recipient.

(5) When sending CUI via email to accounts outside of Federal IT systems the CUI must be in an attachment and protected by encryption or password protection unless the authorized holder assesses that the immediate mission and business needs outweigh any risk of sending the email without encryption or password protection. In such situations, authorized holders may be required by their supervisor to provide a written statement regarding their determination. The password must be transmitted separately from the email attachment containing CUI (e.g., by phone or text).

(6) For phone transmission, encryption is not required. However, authorized holders should consider if the sensitivity of the CUI merits encryption when discussed over the phone. Additionally, CUI Specified may have additional encryption requirements based on a LRGWP.

(7) Only the approved Limited Dissemination Controls listed on the CUI Registry may be applied to limit or specify CUI dissemination. However, authorized holders should be aware of additional dissemination controls that may be authorized or permitted by LRGWP [e.g., UCNI, Export Controlled Information (ECI)].

(8) CUI Privacy information maintained in Privacy Act systems of records may be subject to additional controls if there is information in the records governed by other CUI categories.

(9) The presence or marking of documents and matter containing CUI does not impact the review or release of the document and matter under the Privacy Act (5 USC 552a), FOIA (5 USC 552), or MDRs under EO 13526, Classified National Security Information; and 10 CFR part 1045, *Nuclear Classification and Declassification*. DOE Privacy Act procedures are governed by DOE O 206.1, *Department of Energy Privacy Program*, current version, and DOE FOIA procedures are contained in 10 CFR part 1004. Mandatory Declassification Review Procedures are contained in

10 CFR part 1045 and DOE O 475.2, *Identifying Classified Information,* current version.

(10) When determining whether to disclose information in response to a FOIA, Privacy, or MDR request, the decision must be based on the content of the information and applicability of any FOIA or Privacy equivalencies and exemptions, regardless of whether an agency designates or marks the information as CUI.

(11) All documents and matter must be reviewed to ensure they do not contain CUI prior to public release. CUI must be removed or decontrolled from documents prior to public release.

(12) When intending to share CUI with a non-executive branch entity, there should be a formal agreement whenever feasible. At a minimum, the agreement must include provisions that state:

(a) Non-executive branch entities must handle CUI in accordance with EO 13556, 32 CFR part 2002, this Directive, and the CUI Registry;

(b) Misuse of CUI is subject to penalties established in applicable LRGWP; and

(c) The non-executive branch entity must report any non-compliance with handling requirements to the disseminating office using methods approved by the SAO for CUI.

(13) When an agency cannot enter into agreement but is required to disseminate CUI to non-executive branch entities, it must be communicated to the recipient that the Government strongly encourages the non-executive branch entity to protect CUI in accordance with EO 13556, 32 CFR part 2002, this Directive, and the CUI Registry, and that such protections should accompany the CUI if the entity disseminates it further.

(14) A waiver providing equivalencies and exemptions on encryption can be requested from the Departmental Element's Designated CUI Official. When CUI is reproduced (e.g., copy, scan, print, electronically duplicate) or shared in furtherance of an LGP, it must be marked and protected in the same way as the original CUI document.

(15) When reproducing CUI on equipment such as printers, copiers, scanners, or fax machines, ensure to the extent possible the equipment does not retain the copied data or CUI but may retain other unrelated data, and that the equipment is sanitized in accordance with NIST (SP) 800-53 and NIST SP 800-88. Consideration should be given to a phased implementation on procuring the required equipment authorized to hold CUI.

d. Destruction.

(1) The decision to dispose of any DOE or NNSA document, whether it contains CUI information or not, must be managed in accordance with its NARA approved records schedule, consistent with the policies and procedures for records disposition, as outlined in DOE O 243.1, *Records Management Program,* current version.

(2) Destruction of CUI, including paper copy or stored in any electronic form/ format (e.g., removable media, backup systems, cloud), must be accomplished according to a NARA approved records schedule, and if determined to be a temporary record, should be disposed of in a manner that makes it unreadable, indecipherable, and irrecoverable. When CUI Specified information is to be destroyed and the applicable LRGWP specifies destruction requirements, the LRGWP must be followed.

(3) Electronic media must be destroyed in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, or successor standard and NIST SP 800-88, or successor standard. It may also be destroyed through any method of destruction approved for Classified National Security Information (32 CFR 2001.47 or any implementing or successor guidance).

(4) For paper destruction, one of two methods must be used: single-step paper destruction or multi-step paper destruction methods.

(5) For the single-step paper destruction method, agencies must:

(a) Employ cross-cut shredders that produce 1 mm x 5 mm (0.04 in. x 0.2 in.) particles (or smaller); or

(b) Pulverize / disintegrate paper using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. (National Institute of Standards and Technology (NIST) SP 800-88, Rev 1, *Guidelines for Media Sanitization*, Table A-1: Hard Copy Storage Sanitization)

(6) The National Security Agency (NSA) maintains an Evaluated Products List (EPL) of equipment that is authorized for destroying hard copy (paper) Classified National Security Information. This equipment also meets CUI single-step paper destruction standards. The most updated NSA EPL for paper shredders can be found at: https://www.nsa.gov/.

(7) Crosscut shredders purchased prior to the issuance of this Directive and not identified on the NSA EPL, may continue to be used for the destruction of CUI paper matter and non-paper products, excluding microfilm. However, these shredders must be replaced once they become unserviceable or after 5 years after the effective date of this Order.

(8) The multi-step paper destruction method may also be used. See Information Security Oversight Office (ISOO) CUI Notice 2019-03: *Destroying Controlled Unclassified Information (CUI) in Paper Form*, or successor guidance, for specific requirements on the single-step and multi-step paper destruction methods.

(9) If there is a lack of capability to destroy CUI as outlined in this Directive, then an exemption or equivalency may be requested from the Departmental Element Designated CUI Official in order to pursue an alternative destruction method.

e. Marking. Detailed marking requirements are contained in the CUI Marking Handbook on the CUI Registry. The CUI Marking Handbook and the CUI Registry can be found at https://www.archives.gov/.

(1) Documents marked under LRGWP are not considered legacy documents and do not need to be reviewed or re-marked except as required under LRGWP. Other documents and matter generated prior to issuance of this Directive or that are maintained in files to which access is restricted (e.g., personnel files) are not required to be reviewed and brought to current standards unless they (or a copy of such document and matter) is/are removed from restricted access files and not to be returned; are distributed outside of DOE; or if a new document and matter is created using information from a legacy document and matter that qualifies as CUI. If any of these conditions are met, then legacy markings must be removed or redacted, the document and matter reviewed, and then re-marked as CUI (if applicable), even if the information was under a legacy material marking equivalency and exemption prior to re-use. In the event legacy documents and matter are not designated or re-marked but are distributed outside of DOE, an equivalency and exemption from the SAO for CUI may be sought to utilize Standard Form (SF) 901 as the cover sheet to indicate that the legacy documents and matter contain CUI. SF 901 may be found at https://www.gsa.gov/.

(2) Documents and matter (including legacy documents and matter) whose marking is governed by a LRGWP must continue to be marked as required under the LRGWP.

(3) When information is designated as CUI, but it is determined that marking it as CUI is excessively burdensome, an equivalency and exemption can be requested from the Departmental Element's Designated CUI Official. If marking information as CUI requires cost and resource considerations that Departmental Elements may not be able to address, then it can be deemed as excessively burdensome. The request must include a rationale for the equivalency and exemption and alternate steps to be taken to ensure sufficient protection. However, if information that is designated as CUI is transmitted to another Departmental Element, it must be appropriately

marked as CUI. If it is excessively burdensome to mark every document and matter being sent to another Departmental Element within DOE, then the SF-901 cover sheet can instead be used to indicate there is CUI within the document and matter. Only the CUI EA-approved cover sheet, SF 901, may be used with no substitutes.

(4) CUI in physical form must be maintained in a controlled environment and is not required to be brought to current marking standards unless removed or transmitted outside of the controlled space. However, any document and matter removed from these controlled environments and not to be returned (or a copy of such document and matter) must be reviewed to determine whether it contains CUI and, if appropriate, marked. A controlled environment is defined as any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

(5) Only CUI markings listed in the CUI Registry are authorized for use when designating unclassified information that requires safeguarding or dissemination controls.

(6) All CUI must be marked with a CUI Banner Marking, which may include up to three elements:

(a) The CUI Control marking consisting of the acronym “CUI”. This is mandatory for all CUI, Basic and Specified.

(b) The CUI Category marking, as published in the CUI Registry. This is mandatory for CUI Specified.

(c) Limited Dissemination Control marking, as published in the CUI Registry. This is not mandatory and should be applied consistent with guidance from the applicable Departmental Element’s Designated CUI Official.

(7) All documents containing CUI must indicate who designated the CUI. At a minimum, the organization originating the information must be identified on the front of the document. In cases where the organization is not sufficient to identify a person with whom to discuss the determination, the name of an individual may also be identified, if appropriate.

(8) When marking decontrolled CUI, the document and matter must clearly indicate that the CUI is no longer controlled when restating, paraphrasing, re-using, releasing it to the public, or donating it to a private institution.

(9) Portion marking is not required.

(10) Special format items (e.g., film, photos, removable media) are required to have CUI markings. In accordance with CUI Notice 2019-01, SF 902 and SF 903 are the authorized labels used to identify the presence of CUI in a special format. The use of these SF is optional. SF 902 and SF 903 may be found at https://isoo.blogs.archives.gov/. Alternate marking/accountability shall be determined by the Departmental Element Designated CUI Official when applying CUI marking is not feasible.

(11) The use of cover sheets is optional unless directed by the Departmental Element Designated CUI Official. Any person who designates documents and matter as CUI may use cover sheets for CUI. Cover sheets may be used to identify CUI, alert observers that CUI is present from a distance, and serve as a shield to protect the attached CUI from inadvertent disclosure. Only the CUI EA-approved cover sheet, SF 901, may be used. SF 901 may be found at: https://www.gsa.gov/. Regardless of the use of cover sheets, documents and matter containing CUI must still be marked as required.

(12) To the extent possible, avoid commingling National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD), or Transclassified Foreign Nuclear Information (TFNI) with CUI in the same document and matter.

(13) Under 10 CFR part 1045, CUI markings are not required for documents containing RD or FRD that are not portion marked.

(14) When it is not practical to avoid commingling and CUI is contained in documents and matter containing NSI, RD, FRD, TFNI that are portion marked, the requirements of 32 CFR part 2002, CUI Notice 2018-05, and 10 CFR part 1045 apply as follows:

(a) A warning/informational box or section on the cover or first page of the classified document to convey that CUI is present in the document and matter with a statement that reads, “This document and matter contains CUI [List all CUI Specified categories and limited dissemination control markings], and must be reviewed and appropriately marked when declassified under DOE O 475.2B, *Identifying Classified Information*."

(b) For portions containing CUI, any limited dissemination instruction(s) must be indicated and for Specified CUI, the appropriate category(ies) must be included.

(c) For portion marked RD, FRD, or TFNI documents commingled with CUI, if decontrol instructions apply, the decontrol instructions must not appear on the front page. Where they appear, decontrol

instructions must clearly be labeled as decontrol instructions for the CUI portions only.

(15) CUI documents and matter that are expected to be revised prior to the preparation of a finished product for dissemination or retention (e.g., all documents to include: Draft, Pre-decisional, etc.) must be marked with the date created or the date of the last change and with "CUI" and any CUI Specified contained in the document and matter. If not destroyed, the document and matter must be marked as final when:

(a) Released by the originator outside the originating activity;

(b) Retained more than 180 days from the date of origin or last change; or

(c) Filed according to the applicable records control schedule.

(16) The following administrative markings may be used for CUI within DOE. No other administrative markings may be used unless approved and promulgated within DOE by the DOE SAO for CUI:

(a) Predecisional

(b) Deliberative

(c) Draft

(d) Must be reviewed prior to public release

(17) Email messages must include a Banner Marking to indicate that the email contains CUI. If the message itself is not CUI but contains an attachment with CUI, the message must indicate that the attachment is CUI and that when separated the email does not contain CUI. The attachment must have all required CUI markings.

(18) Scientific and Technical Information (STI) documents and matter being submitted to the Office of Scientific and Technical Information (OSTI) for subsequent announcement, availability, and preservation, in accordance with DOE O 241.1, *Scientific and Technical Information Management*, current version, should be appropriately marked. Inform OSTI when STI previously announced or submitted to OSTI has been modified.

(19) If a determination to change the CUI marking (which would include adding or removing limited dissemination controls) further limits access to the document, to the extent possible, the person making the change must notify persons to whom the document was distributed to of the change, to ensure the information is not provided to unauthorized persons. There is no need for notification unless the change impacts access.

(20) Documents from closed or inactive sites should be reviewed and re-marked or decontrolled by the document custodian before distributing to another DOE entity or releasing it to the public.

f. Safeguarding. Safeguarding requirements for CUI depend on whether the CUI is Basic or Specified. CUI Specified must be safeguarded in accordance with requirements in applicable LRGWP. If safeguarding requirements are not addressed in LRGWP (e.g. CUI Basic), there must be reasonable precautions to guard against unauthorized disclosure of CUI. At a minimum, safeguarding measures must include the following precautions:

(1) Safeguard CUI documents and matter in accordance with the requirements of this Directive and the underlying LRGWP as indicated in the CUI Registry.

(2) Establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments.

(3) Reasonably ensure that unauthorized individuals cannot access or observe CUI. To the extent possible, ensure unauthorized individuals cannot inadvertently overhear conversations discussing CUI.

(4) Keep CUI under authorized holder's direct control or protect it with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment. Examples of physical barriers include: sealed envelopes and areas equipped with electronic locks. Additionally, locked doors, overhead bins, drawers, and file cabinets can also serve as a physical barrier.

(5) CUI may be processed, stored, or transmitted on both federal information systems operated by DOE and by a contractor on behalf of DOE. Because the confidentiality impact value for CUI is no lower than moderate in accordance with FIPS Publication 199, systems containing CUI must ensure proper controls are implemented according to NIST SP 800-53 Rev 5, or successor standard, in alignment with 205.1C, *Department of Energy Cybersecurity Program,* current version.

(6) CUI stored on non-federal information systems must follow the requirements of NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, in order to protect CUI, unless specific requirements are specified by LRGWP for protecting the information.

(7) Ensure that if an unmarked document and matter is believed to contain CUI, the unmarked document and matter is protected as CUI until it can be reviewed to determine if it contains CUI.

(8) Legacy documents and matter that will retain Official Use Only (OUO) markings or have not been reviewed to determine if they contain CUI should also be safeguarded in accordance with the requirements established in this Directive. If safeguarding requirements cannot be met, alternate plans for appropriately protecting documents and matter that may potentially contain CUI must be developed. This alternate protection plan must be approved by the Departmental Element Designated CUI Official or delegate.

(9) Permanent burial is an option that may be approved by the Departmental Element Designated CUI Official for permanent placement of CUI materials, excluding records.

g. CUI Training.

(1) All employees who have access to CUI must be trained on appropriate handling procedures and requirements within six months after the CUI Training Program becomes available and once every two years thereafter.

(2) New employees who have access to CUI, including interns and those on short-term detail and assignments, must be trained upon initial employment and once every two years thereafter.

(3) CUI training will address the following CUI items and activities from a DOE-wide perspective:

(a) Identification;

(b) Marking;

(c) Access;

(d) Transmission;

(e) Protection;

(f) Destruction; and

(g) Challenges.

(4) Any employee who has access to or marks CUI must receive training on designating CUI, relevant CUI categories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures.

h. Decontrolling CUI.

(1) Documents and matter marked as containing CUI must be reviewed by the disseminating office prior to public release to ensure it does not contain CUI by removing the CUI, decontrolling the CUI, or determining that the information is not exempt from public release, and the CUI markings must be removed.

(2) Unless decontrol authority is governed by LRGWP, only the disseminating office can decontrol documents and matter marked as containing CUI, and must coordinate decontrolling with other cognizant offices, when necessary.

(3) Transferring records to NARA.

(a) When feasible, records containing CUI must be decontrolled prior to transferring to NARA.

(b) When records cannot be decontrolled before transferring to NARA, it must be indicated on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI (subject to NARA's regulation on transfer, public availability, and access: See 38 CFR parts 1235, 1250, and 1256).

(c) For hard copy transfer, do not place a CUI marking on the outside of the container.

i. Self-Inspection.

(1) There must be an annual self-inspection of the DOE CUI Program. This will be conducted through the CUI SAO selection of a group of Departmental Elements to serve as a representative sample of the entire Department. Each year, there will be a new group of Departmental Elements selected. Self-inspections will occur through predictive cycles.

(2) Program Assessments.

(a) The Departmental Element Designated CUI Official ensures the annual assessment is conducted.

(b) Annual assessment of the CUI program must evaluate the following:

1 Training,

2 Identification,

3 Marking, and

4 Safeguarding.

(3) Self-inspections of the CUI program of the Office of Inspector General (OIG) can only be conducted by OIG personnel.

j. Challenges.

(1) DOE personnel who, in good faith, believe that designation of CUI is improper or incorrect, or who believe they have received unmarked CUI, may submit a challenge to their Departmental Element Designated CUI Official.

(2) For information not under the Departmental Element's cognizance, ensure the challenge is submitted to the appropriate authority. Challenges for Specified CUI are submitted under the requirements and authorities established under the applicable LRGWP or DOE Directive.

(3) There must be a process within each Departmental Element to accept and manage challenges to CUI status. The process must include referral of challenges governed by LRGWP or a DOE Directive to the appropriate authority. Challenges may be issued by anyone in DOE without fear of reprisal or retribution, with the challenged information protected from broad disclosure. Otherwise, the process must include a timely response to the challenger that:

(a) Acknowledges receipt of the challenge;

(b) States an expected timetable for response to the challenger;

(c) Requires the challenger to define a rationale for belief that the CUI in question is inappropriately designated;

(d) Gives contact information for the official making the Departmental Element’s decision in this matter;

(e) Ensures there is no retribution for challenges; and

(f) Until the challenge is resolved, ensures the challenged CUI is safeguarded and disseminated at the control level indicated in the markings.

If the challenged document or matter is not marked as CUI, it should be treated as CUI until the challenge is resolved.

(4) Except as governed by the requirements and authorities under LRGWP, if a challenger disagrees with the Departmental Element response, the

challenger may first appeal to the DOE CUI SAO. If the issue is still not resolved, then the challenger may use the Dispute Resolution procedures described in 32 CFR part 2002.

k. Misuse.

(1) Misuse of CUI, in printed or electronic form, must be reported in accordance with the requirements provided in this Directive to the Departmental Element Designated CUI Official.

(2) Incidents of misuse are reported following security incident and/or incident response timelines and procedures developed by the Departmental Element.

(3) Any misuse of CUI Specified may be considered as an Incident of Security Concern under DOE O 470.4, *Safeguards and Security Program,* current version.

(4) Incidents of misuse of CUI must be reported and investigated if the misuse results in the information being released to unauthorized persons.

5. RESPONSIBILITIES.

a. Secretary of Energy (S1). Designates the DOE SAO for CUI.

b. DOE SAO for CUI.

(1) Designated in writing by the Secretary as the SAO for CUI responsible for implementing the CUI Program. Serves as the primary point of contact for official correspondence, accountability reporting, and other matters of record between DOE and the CUI EA.

(2) Designates the CUI Program Manager.

(3) Establishes agency processes and criteria for reporting and investigating misuse of CUI as defined in 32 CFR section 2002.4 and in accordance with section 2002.54 to the CUI Program. These processes and criteria are in addition to any other reporting or investigating obligations and authorities, such as those established for the OIG.

(4) Establishes an authority which takes administrative action against misuse of CUI.

(5) Approves DOE-wide CUI Training Program and consults with the National Training Center (NTC) in the development of CUI Training Program in accordance with the training requirements under 32 CFR part 2002.

(6) Except as governed by LRGWP, reviews Departmental Element-approved exemptions and equivalencies to maintain visibility over exemptions and equivalencies of all or some of the CUI marking and safeguarding requirements while the CUI remains within DOE control.

(7) Ensures exemptions and equivalencies requested for CUI governed by LRWGP are referred to the appropriate authority.

(8) Maintains final approval authority over all CUI exemptions and equivalencies over CUI marking and safeguarding requirements while the CUI remains within DOE control and coordinates exemptions and equivalencies with NARA as necessary.

(9) Annually reviews and assesses DOE's CUI Program to ensure program effectiveness, measures the level of compliance, and monitors the progress of CUI implementation across DOE. This will be conducted through an annual self-inspection by selecting a group of Departmental Elements to serve as a representative sample of the entire Department.

(10) Sets proper controls and countermeasures necessary to protect information on Information Technology (IT) systems during processing, while in storage, and during transmission, per FIPS 199 and NIST SP 800-53.

c. CUI Program Manager.

(1) Serves as the official representative to the CUI EA on DOE's day-to-day CUI Program operations, both within the DOE and in interagency contexts.

(2) Has overall responsibility for managing CUI requests and concerns from Departmental Elements.

(3) Serves as the CUI liaison between the Office of the Chief Information Officer (OCIO) and the Departmental Elements.

d. Heads of Departmental Elements.

(1) Implement the CUI program, to include training, within their Departmental Elements.

(2) Ensure oversight of CUI complies with DOE O 226.1, *Implementation of Department of Energy Oversight Policy,* current version.

(3) Designate in writing a Departmental Element Designated CUI Official and notifies the CUI SAO of the appointment and any changes.

(4) Ensure Departmental Element processes that align with the requirements listed in this Directive are in place for reporting and investigating misuse of CUI.

(5) Ensure the requirements and responsibilities of this Directive are followed by all their subordinate organizational levels.

(6) Identify additional requirements covering the sections listed above for any CUI Specified Categories owned or managed by the Departmental Element.

(7) Recommend additional supplemental administrative markings to the Departmental Element's Designated CUI Official.

(8) Determine if element-specific training is required for their personnel as a supplement to the DOE-wide CUI training program.

e. Departmental Element Designated CUI Official.

(1) Oversees the implementation of the requirements in this Directive within their element in compliance with DOE O 226.1, *Implementation of Department of Energy Oversight Policy,* current version.

(2) Determines the individual(s) responsible for approving and complying with the single-step and multi-step destruction process.

(3) Except as governed by LRGWP, approves exemptions and equivalencies of all or some of their Element's CUI marking, safeguarding, and destruction requirements while the CUI remains within DOE control and reports approved exemptions and equivalencies to the SAO for CUI.

(4) Approves requests for additional approved methods of public release and reports approved requests to the SAO for CUI.

(5) Collaborates with NTC on CUI Specified training requirements when warranted for Departmental Element employees in accordance with this Directive and ensures element employees receive appropriate NTC CUI training.

(6) Develops and maintains a list of CUI Basic and Specified Categories most applicable to the Departmental Element for persons within the element to reference when identifying and marking CUI.

(7) Submits requests for new CUI Categories to the DOE SAO for CUI.

(8) Creates a process within their Departmental Element to accept and manage challenges and reports of misuse, to include referral to appropriate authorities under LRGWP.

(9) Except as governed by LRGWP, determines alternate markings / accountability in coordination with the cognizant office (when applicable) when applying CUI marking is not feasible.

(10) May appoint internal program and contractor liaisons to support the Departmental Element Designated CUI Official in addressing inquiries and communicating CUI Program updates to Authorized Holders.

(11) Reviews requests for permanent burial as an option for permanent placement of CUI materials, excluding records.

f. Authorized Holders.

(1) Safeguard CUI in all forms including written, verbal, and electronic in accordance with the requirements of this Directive and the applicable LRGWP as indicated in the CUI Registry.

(2) Challenge information they believe is improperly or incorrectly identified as or is not identified as CUI, as appropriate.

(3) Report the misuse of CUI under their Departmental Element's procedures, in printed or electronic form.

(4) Complete CUI training required under this Directive and applicable LRGWPs.

(5) Comply with 32 CFR part 2002 and applicable LRGWPs.

(6) Coordinate with the appropriate authorities as necessary.

g. National Training Center (NTC).

(1) Develop the training program in accordance with the training requirements set forth in 32 CFR part 2002 and in consultation with the DOE SAO for CUI.

(2) Maintain and update the training related to CUI, as necessary.

(3) Provide training to Departmental personnel.

(4) Assist in the development of the CUI Specified training.

6. INVOKED STANDARDS. The following DOE technical standards and industry standards are invoked as required methods in this Order in accordance with the applicability and conditions described within this Order. Any technical standard or industry standard that is mentioned in or referenced by this Order, but is not included in the list below, is not invoked by this Order. Note: DOE O 251.1D, Appendix J provides a definition for "invoked technical standard."

a. NIST FIPS 140-3, *Security Requirements for Cryptographic Modules*. This standard requires the use of compliant encryption methods for the transmission of CUI over the internet, including email transmission, fax transmission, printing, copying, removable media, and storage on shared drives, and with collaboration tools such as text messaging, video conferencing, and other productivity tools.

b. NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. This standard is required to be used to ensure that CUI is processed, stored, or transmitted on both federal information systems operated by DOE and by a contractor on behalf of DOE at a confidentiality impact value no lower than moderate.

c. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This standard is required to be used to set the proper controls and countermeasures necessary to protect information on Information Technology (IT) systems during processing, while in storage, and during transmission, as well as ensuring the proper destruction of Electronic media.

d. NIST SP 800-88, *Guidelines for Media Sanitization*. This standard is required to be used to ensure when reproducing CUI on equipment such as printers, copiers, scanners, or fax machines, that the equipment does not retain the copied data or CUI, and that the equipment is sanitized accordingly. Additionally, this standard is required to be used when destroying electronic media containing CUI.

e. NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. This standard is required to be used in order to protect CUI stored on non-federal information systems.

7. REFERENCES.

a. Executive Order (EO) 13556, Controlled Unclassified Information

b. Title 32 Code of Federal Regulations (CFR), part 2002, *Controlled Unclassified Information*

c. Title 10 CFR, part 1017, Identification and Protection of Unclassified Controlled Nuclear Information

d. H.R.624, Social Security Number Fraud Prevention Act of 2017

e. DOE Order (O) 205.1, Department of Energy Cybersecurity Program, current version

f. DOE O 206.1, Department of Energy Privacy Program, current version

g. DOE O 221.1, Reporting Fraud, Waste and Abuse to the Office of Inspector General, current version

h. DOE O 221.2, Cooperation with the Office of Inspector General, current version

i. DOE O 226.1, Implementation of Department of Energy Oversight Policy, current version

j. DOE O 243.1, *Records Management Program*, current version

k. DOE O 241.1, Scientific and Technical Information Management, current version

l. DOE O 251.1, Departmental Directives Program, current version

m. DOE O 470.4, Safeguards and Security Program, current version

n. DOE O 471.1, Identification and Protection of Unclassified Controlled Nuclear Information, current version

o. DOE O 471.6, *Information Security*, current version

p. DOE O 475.2, Identifying Classified Information, current version

8. DEFINITIONS. Attachment 2 provides definitions.

9. CONTACT. Questions concerning this Directive should be directed to the Office of the Chief Information Officer at (202) 586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT DOE O 471.7, *CONTROLLED UNCLASSIFIED INFORMATION*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD and the applicable requirements in Executive Order (EO) 13556, 32 Code of Federal Regulations (CFR) part 2002, and the CUI Registry. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachment 2 to DOE O 471.7, referenced in and made a part of this CRD, which provides information applicable to contracts in which this CRD is inserted.

1. Nothing in this CRD is intended to restrict the creation or dissemination of unclassified scientific research, in alignment with the scientific missions of DOE, NSDD-189, the OPEN Government Act of 2007 (Public Law No: 110-175) and the OPEN Government Data Act (Title II of the Foundations for Evidence-Based Policymaking Act (Public Law 115-435).

2. The Contractor must institute a Controlled Unclassified Information (CUI) Program consistent with Departmental Element and Site Office federal direction for the appropriate identification, marking, safeguarding, dissemination, decontrolling, and destruction of CUI. The Contractor's CUI program must ensure that:

    a. Applicability. CUI standards are applied to all federal unclassified information. Only those categories approved by National Archives and Records Administration (NARA), the CUI Executive Agent (EA), and published in the CUI Registry are used to identify, mark, safeguard, disseminate, decontrol, and destroy CUI.

    b. Identification. Federal unclassified information created or originated by the contractor, produced by or for the contractor, or under the control of the contractor, through a DOE contractual mechanism, that has been determined to be CUI [per Departmental Element direction or law, regulation, or government-wide policy (LRGWP)], is identified as containing CUI.

    c. Marking. Documents and matter determined to contain CUI are marked appropriately as defined in the CUI registry. Except for Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI), CUI markings are the only markings to be used to designate documents and matter containing CUI.

    d. Communication. The Office of Scientific and Technical Information (OSTI) is notified when there are modifications to the CUI status of scientific and technical information previously announced or submitted to OSTI, in accordance with DOE O 241.1, *Scientific and Technical Information Management*, current version.

e. Safeguarding.

(1) CUI may be processed, stored, or transmitted on both federal information systems operated by DOE and by a contractor on behalf of DOE. Because the confidentiality impact value for CUI is no lower than moderate in accordance with federal Information Processing Standards Publication 199, systems containing CUI must ensure proper controls are implemented according to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 in alignment with DOE Order (O) 205.1, *Department of Energy Cybersecurity Program,* current version.

(2) CUI stored on non-federal information systems must follow the requirements of NIST SP 800-171 in order to protect CUI, unless specific requirements are specified by LRGWP for protecting the information.

(3) Program must establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments. A controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure. When outside a controlled environment, ensure CUI is protected under authorized holder's direct control, or with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation.

(4) Program must ensure that if an unmarked document and matter is believed to contain CUI, the unmarked document and matter is protected as CUI until it can be reviewed to determine if it contains CUI.

(5) CUI that is reproduced (e.g., copied, scanned, printed, electronically duplicated) or shared must be protected the same as the original CUI document and matter in furtherance of a Lawful Government Purpose (LGP).

(6) When reproducing CUI on equipment such as printers, copiers, scanners, or fax machines, ensure to the extent possible the equipment does not retain the unencrypted copied data or CUI but may retain other unrelated data, and that the equipment is sanitized. Consideration should be given to a phased implementation of eventually requiring all equipment authorized to hold CUI to meet this requirement.

f. CUI Training. Contractors interacting with CUI documents and matter shall receive training approved by the Departmental Element Designated CUI Official or delegate.

g. Access and Sharing. Access to documents and matter marked as containing CUI or CUI from such documents and matter are provided only to those persons who

have a LGP. Additionally, access to CUI is restricted in accordance with applicable LRGWP.

h. Dissemination. [Limits on how CUI is transmitted.]

(1) When sending CUI via email to accounts outside of Federal IT systems the CUI must be in an attachment and protected by encryption or password protection unless the authorized holder assesses that the immediate mission and business needs outweigh any risk of sending the email without encryption or password protection. In such situations, authorized holders may be required by their supervisor to provide a written statement regarding their determination. The password must be transmitted separately from the email attachment containing CUI (e.g., by phone or text).

(2) Legacy documents and matter that will retain Official Use Only (OUO) markings or have not been reviewed to determine if they contain CUI, should also be safeguarded in accordance with the requirements established in this CRD. If safeguarding requirements cannot be met, the Contactor must develop alternate plans for appropriately protecting documents and matter that may potentially contain CUI. This alternate protection plan must be approved by the Departmental Element Designated CUI Official or delegate.

i. Decontrol.

(1) Documents and matter determined by the disseminating office to no longer warrant protection as CUI shall have their markings removed. Decontrol instructions are not required, but if known, may be indicated on the front of the document.

(2) Transferring records to NARA.

(a) When feasible, records containing CUI must be decontrolled prior to transferring to NARA.

(b) When records cannot be decontrolled before transferring to NARA, it must be indicated on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI (subject to NARA's regulation on transfer, public availability, and access: See 38 CFR parts 1235, 1250, and 1256).

(c) For hard copy transfer, do not place a CUI marking on the outside of the container

j. Destruction. Destruction of CUI, including in electronic form, is accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable.

k. Equivalency and Exemption. Any request for an equivalency or exemption from any requirements in the CRD for DOE O 471.7 must be provided to the appropriate Departmental Element Designated CUI Official or designee. Such requests must:

(1) Identify the requirement for which an equivalency or exemption is being requested,

(2) Explain why the equivalency or exemption is needed, and

(3) If requesting an equivalency or exemption, describe the alternate or equivalent means for meeting the protection requirements.

l. Misuse. Reports on certain types of CUI misuse, only if the misuse may result in the document being released to unauthorized persons, are reported to the Departmental Element and Site Office Designated CUI Officials as soon as is practical, and to the OIG, as necessary pursuant to OIG reporting requirements. The types of reportable misuse include:

(1) CUI from a document and matter marked as containing CUI is intentionally released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE-authorized activities.

(2) A document and matter marked as containing CUI is intentionally or negligently released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE-authorized activities.

(3) A document and matter that is known to contain CUI is intentionally not marked.

(4) A document and matter that is known to not contain CUI is intentionally marked as containing such information.

If the reports result in violations being confirmed, then the Contractor will self-impose penalties, as appropriate. Moreover, the Departmental Element may make a determination on additional Contractor penalties.

ATTACHMENT 2: DEFINITIONS

This Attachment provides information and/or requirements associated with DOE O 471.7 as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 471.7) is inserted.

1. Access. Granting permission to view and handle CUI, provided such access or dissemination: (i) Abides by the laws, regulations, or Government-wide policies that established the CUI category; (ii) Furthers a lawful Government purpose; (iii) Is not restricted by an authorized limited dissemination control established by the CUI EA; and (iv) Is not otherwise prohibited by law.

2. Authorized Holder. An individual, organization, or group of users that is permitted to designate or handle CUI, consistent with the guidelines in this Directive, 32 CFR Part 2002, and the CUI Registry.

3. Control Level. A general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

4. Controlled Environment. Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

5. Controlled Unclassified Information (CUI). CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a LRGWP requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

6. CUI Basic. This is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.

7. CUI Categories. Types of information for which a LRGWP requires or permits agencies to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the CUI Registry. The controls for any CUI Basic categories are the same, but the controls for CUI Specified categories can differ from CUI Basic ones and from each other. A CUI category may be CUI Specified, and vice versa. If dealing with CUI that falls into a CUI Specified category, review the controls for that category on the CUI Registry. Also consult the agency's CUI policy for specific direction from the SAO for CUI.

8. CUI Executive Agent (EA). The Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) is designated as the U.S. Government CUI EA for the executive branch and issues guidance to all Federal agencies on safeguarding and marking CUI.

9. CUI Specified. This is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic.

10. CUI Marking Handbook. A resource that provides additional guidance on CUI Marking instructions. This handbook is publicly available on the CUI Registry.

11. CUI Registry. The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this Directive. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. The CUI Registry also indicates which LRGWP include any specific requirements for CUI Specified.

12. Decontrolling. An event that occurs when the disseminating office, consistent with this Directive and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action.

13. Disseminating Office. The Office responsible for identifying and marking a document and matter as CUI.

14. Electronic Media. Consists of devices containing bit / bytes like hard drives, random access memory, read only memory, disks, memory devices, etc.

15. Export Controlled Information. Information (which may include technology, technical data, assistance or software), the export (including, as applicable, transfer to foreign nationals within the United States) of which is controlled under the "Export Administration Regulations" (maintained by the U.S. Department of Commerce), the "International Traffic in Arms Regulations" (maintained by the U.S. Department of State), "10 CFR Part 810, Assistance to Foreign Atomic Energy Activities" regulations (maintained by the U.S. Department of Energy), or various trade and economic sanctions (maintained by the U.S. Department of Treasury's Office of Foreign Assets Control).

16. Handling CUI. Any use of CUI, including but not limited to identifying, marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

17. Hard Copy Media. Physical representations of information such as paper, faxes, ribbons, drums, etc.

18. Lawful Government Purpose (LGP). Lawful Government Purpose, as defined by the CUI Registry, is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement). An employee's LGP may be defined by DOE policy, position descriptions, or contractual requirements.

19. Law, Regulation, or Government-wide Policy (LRGWP). The basis for safeguarding or dissemination controls under 32 CFR part 2002.

20. Legacy Material. Unclassified information (e.g., OUO) that is marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

21. Limited Dissemination Control. Is any CUI EA-approved control that agencies may use to limit or specify CUI dissemination. (e.g., Dissemination List Controlled (DL Only)).

22. Misuse of CUI. Results in the release of a document and matter containing CUI to unauthorized persons.

23. Scientific and Technical Information (STI). Information products deemed by the originator to be useful beyond the originating site (i.e., intended to be published or disseminated), in any format or medium, which contain findings and technological innovations resulting from research and development (R&D) efforts and scientific and technological work of scientists, researchers, and engineers, whether Federal employee, contractor, or financial assistance recipient. STI also conveys the results of demonstration and commercial application activities as well as experiments, observations, simulations, studies, and analyses. Scientific findings are communicated through various media – e.g., textual, multimedia, audiovisual, and digital – and are produced in a range of products such as technical reports, scientific/technical conference papers and presentations, theses and dissertations, scientific and technical computer software, journal articles, workshop reports, program documents and matter, patents, publicly available scientific research datasets, or other forms of STI. STI may be classified, Unclassified Controlled Nuclear Information (UCNI), controlled unclassified information (CUI), or unclassified with no access restrictions. DOE-funded STI originates primarily from research and other activities performed by site/facility management contractors, direct DOE-executed prime procurements, DOE-operated research activities, and financial assistance recipients, in addition to DOE employees.