Reclamation Manual

Directives and Standards

Subject: Identifying and Safeguarding Controlled Unclassified Information (CUI)

Purpose: Describes the requirements and procedures for identification and safeguarding sensitive but unclassified information referred to herein as CUI. The benefits of this Directive and Standard (D&S) are to provide standard instructions on sensitive but unclassified information. In addition, this D&S helps to align the Bureau of Reclamation with other governmental practices regarding protection of this type of information.

Authority: Reclamation Act of June 17, 1902 (32 Stat. 388; 43 U.S.C. 391) and acts amendatory thereof and supplementary thereto; Safety of Dams Act of 1978 (Pub. L. 95-578) and acts amendatory thereof; Critical Infrastructure Protection Act of 2001 (Pub. L. 107-56; 115 Stat. 272; 42 U.S.C. 5195c); Homeland Security Act of 2002 (Pub. L. 107-296; 116 Stat. 2135; 6 U.S.C. 101); Federal Information Security Management Act of 2002 (44 U.S.C. 3541); Consolidated Natural Resources Act of 2008, Section 513, Bureau of Reclamation Site Security (Pub. L. 110-229; 122 Stat. 755; 43 U.S.C. 373e); 32 CFR Part 2002 Controlled Unclassified Information; Executive Orders (EO) 10450, 10577, 12968, 13526, and 13556; Homeland Security Presidential Directives; Federal Information Processing Standards 200 and 201; and Departmental Manual (DM) Parts 380, 442, 444, and 446.

Approving Official: Director, Mission Assurance and Protection Organization (MAPO)

Contact: MAPO, Security Division (84-57000)

1. Introduction.

The unauthorized disclosure of CUI may impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. This D&S defines the requirements for safeguarding CUI, including draft information, originating within Reclamation. It is also applicable to all CUI information received by Reclamation from non-Reclamation entities, where those entities do not provide specific safeguarding guidance.

2. Applicability.

A. All Reclamation offices and employees.

B. Contractors will follow this D&S when the contract includes Reclamation Acquisitions Regulations WBR 1437.8103 paragraph (b).

C. This D&S is not applicable to classified national security information covered by EO 13526.

3. Responsibilities.

A. Director, MAPO.

The Director, MAPO, working through the Chief Security Officer, is responsible for:

(1) overseeing program activities to identify and safeguard CUI,

(2) providing oversight to ensure compliance with this D&S,

(3) promulgating Reclamation CUI Policy, D&S, and guidance, and

(4) developing and delivering additional training materials and forums to educate employees and others on the proper recognition and safeguarding of CUI.

B. Associate Chief Information Officer (ACIO).

The ACIO is responsible for developing policies and procedures for storage of CUI on Reclamation information technology (IT) systems.

C. Directors, Managers, and Supervisors.

Directors, managers, and supervisors are responsible for:

(1) ensuring compliance with the standards for safeguarding CUI as cited in this D&S,

(2) establishing and maintaining adequate procedures, education, and awareness with emphasis on the safeguarding of CUI and the prevention of unauthorized disclosure, and

(3) taking appropriate corrective actions, to include administrative or disciplinary actions, when violations occur, following Department of the Interior and Reclamation procedures.

D. Regional Security Officer.

Regional security officers are responsible for regional implementation to include, employee awareness, oversight, and providing technical expertise.

E. Employees.

Reclamation employees are responsible for:

(1) awareness of, and complying with, the safeguarding requirements for CUI as outlined in this D&S and other Departmental policy and training.

(2) awareness that divulging information without authority may result in administrative or disciplinary action.

(3) informing their supervisor of any procedures or incidents that may result in the inappropriate disclosure or compromise of CUI.

(4) identifying and marking information that is CUI. Recipients or holders of unmarked Reclamation information who conclude that specific information is to be marked as CUI will protect that information and promptly notify the originator of their determination.

(5) informing any outside entities of the requirements associated with this D&S prior to providing any CUI.

(6) applying the operations security process prior to releasing sensitive information outside of Reclamation.

4. General

A. Records Management.

There are criminal penalties associated with the unlawful removal or destruction of Federal records (18 U.S.C. 2071 and 36 CFR 1228.102). There are also penalties associated with the improper handling of records containing information exempt from disclosure under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Contact your local records manager or FOIA officer for additional identification and handling guidance for Federal records.

B. Sensitive Information.

Information is designated as sensitive to protect, control, and restrict access, as permissible under laws and regulations. The release of such information may cause harm to a person’s privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to our national and agency interests.

C. CUI Designation.

Within Reclamation, a CUI designation will be used to identify all sensitive but unclassified information.

D. CUI Categories and Subcategories.

The CUI Program is founded on the prerequisite that only information requiring protection based in a law, Federal regulation, or government-wide policy can qualify as CUI. Each category and subcategory is based in at least one (and sometimes many) of these laws, regulations, or government-wide policies – also referred to as Authorities – that require a certain type of information to be protected or restricted in dissemination.

(1) Though CUI is divided into categories and subcategories, the handling, control, and protection requirements are the same as outlined in this D&S, unless specifically noted otherwise below.

(2) The official repository for all Category and Subcategory information is: https://www.archives.gov/cui/registry/category-list.

E. FOIA Disclosure.

Information designated as CUI is not automatically exempt from disclosure under the provisions of FOIA (5 U.S.C. 552). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis by the servicing FOIA office.

F. Inappropriate Use of the CUI Designation.

Designation of information as CUI will not be used as a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to the government, its officials, or other personnel.

G. Designation Responsibility.

Reclamation employees have the responsibility to designate sensitive information as CUI. When sharing CUI information with parties outside Reclamation, individuals must ensure the recipients understand Reclamation's CUI requirements and will protect it accordingly.

H. Duration of Designation.

Information designated as CUI will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

I. Other Agency Information.

CUI from other government agencies, must be handled in accordance with the requirements provided by the other submitting governmental agency. Where no requirements are provided, it must be handled in accordance with the requirements of this D&S.

5. CUI.

A. General Types of CUI.

CUI includes, but is not limited to, the following types of information.

(1) Information of the type that may be exempt from disclosure per FOIA (5 U.S.C. 552), and its amendments.

(2) Information exempt from disclosure per the Privacy Act (5 U.S.C. 552a).

(3) International and domestic information protected by statute, treaty, regulation or other agreements, including proprietary information.

(4) Information that may result in increased harm to personnel, facilities, property, or the public, such as specific security or safety information that may be maliciously exploited if exposed to the general public in an uncontrolled manner.

(5) Internal IT systems data revealing information about:

(a) configurations of servers, desktops, applications, and networks, including: names, versions, and patch levels of applications,

(b) configurations and topologies of network switches, routers, firewalls, and gateways,

(c) significant network interconnections,

(d) carriers and locations of significant communications centers,

(e) deployment of intrusion detection and prevention tools,

(f) access and authentication methods,

(g) vulnerability scan results and firewall rule-sets, and

(h) significance of mission or business need.

(6) Data revealing exploitable infrastructure vulnerabilities or the security posture of a system, subsystem, or infrastructure component. For example, threat or risk assessments, system or facility security plans, contingency plans, risk management plans, business impact analysis studies, and assessment and accreditation documentation associated with a Reclamation IT system.

(7) Reviews or reports illustrating or disclosing exploitable vulnerabilities of persons, systems, or facilities, not otherwise eligible for national security classification.

(8) Information that may constitute an indicator of sensitive U.S. Government intentions, capabilities, operations, activities, or otherwise threaten operations. This includes, but is not limited to, industrial control system state information and alarm parameters and conditions, including system screenshots.

(9) Developing or current technology, the release of which could hinder the objectives of Reclamation, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

(10) Internal financial, budget, acquisition, or draft policy information that would not be appropriate for public disclosure until deemed finalized and releasable.

(11) Certain research and development information where such information reveals vulnerabilities, results in risk to personnel or property, or constitutes the intellectual property of a non-Federal entity or individual.

(12) Information associated with cyber assets and their associated security controls, as designated by Reclamation in support of the NERC-CIP standards.

B. Specific Examples of Reclamation CUI.

(1) Examples of Reclamation CUI are given in Appendix A. Appendix A only provides examples and is not intended to serve as an all-inclusive list. The context of the information must always be taken into account when determining if the information is actually sensitive.

(2) If you believe information is CUI, but it is not listed as one of the examples, consult with your supervisor or your directorate's security team before applying CUI markings and control measures.

6. General Required Handling Procedures.

A. Marking.

(1) Information designated as CUI will be sufficiently marked and safeguarded, as outlined below, so that persons having access to it are aware of its sensitivity and safeguarding requirements. All holders will protect CUI accordingly, even information not properly marked.

(2) These marking procedures apply to all newly-developed CUI and any existing unmarked information determined to be CUI. Existing information does not require new marking until the information is distributed or released. Information that has been previously marked as sensitive information (e.g., FOUO) shall be

remarked before distribution if it is feasible to do so (for example, the markings can be changed before reprinting).

(a) Prominently mark the center top and bottom of the front cover, first page, title page, and each individual page containing CUI with "CONTROLLED" in black, bold, capital letters, large enough to be readily visible to the casual reader. (See Appendix C.)

(b) Designator or originator information and markings, decontrol instructions (see 7.E), and date/event markings shall be included on the first page and/or cover sheet. For example: "Controlled by: Division 5, Department of Good Works. Decontrol by: date, occurrence of special event, or do not decontrol." (See Appendix C.)

(c) Cover sheets (OF-901) must be used for documents transmitted outside Reclamation. (See Appendix B.) Coversheets on internal documents are optional, but recommended.

(d) Computer storage media, e.g., disks, tapes, CDs/DVDs, removable drives, etc., containing CUI will be marked "CONTROLLED" or "CUI" and "Reclamation" with permanent marker, label, or stamp.

(e) Individual portion or paragraph markings are optional, but recommended, on a document that contains CUI or a mix of CUI and non-sensitive information.

(f) Individual portions or paragraphs of a classified document where the portion or paragraph contains only CUI will be marked (CUI); classified portions will be marked in accordance with the applicable classification guide and classified marking standards.

B. Dissemination and Access.

(1) As required by 32 CFR Part 2002, CUI must only be shared with outside entities if a non-disclosure agreement has been signed; Reclamation does not consider managing partners to be outside entities. Non-disclosure agreements do not apply to other Reclamation employees and must not conflict with any Prohibited Personnel Practices. (Reclamation's official NDA form is included in Appendix D.)

(2) Access to CUI will be limited and, on a need,-to-know basis as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his/her supervisor or the information's originator.

(3) CUI will not be disseminated in any manner—orally, visually, or electronically—to individuals or organizations not performing or assisting in a lawful and authorized specific government function and not having an appropriate need-to-know, with the exception of approved FOIA requests. Holders of information do not have permission to give blanket or general access to CUI for convenience. Reclamation must assign individuals in an organization an official Government task, specifically related to the accessed information.

(4) Information requested by the public under a FOIA request must be reviewed on a case-by-case basis by the servicing FOIA office in coordination with the originator of the information, subject matter expert, or the technical office responsible for the type of information requested to determine if the information is releasable under FOIA.

(5) A security clearance or background investigation is not required for need-to-know access to CUI.

(6) When discussing or transferring CUI to another individual, the holder must ensure precautions are taken to prevent unauthorized compromise of the protected information, such as ensuring that discussions do not take place where they may be overheard by those without a need-to-know.

(7) If a transmittal document is included with the CUI, it will conspicuously include the following instructions: "When enclosure is removed, this transmittal document is not CUI."

(8) If the protected information being disseminated belongs to another agency or organization, Reclamation will comply with their policies concerning further dissemination. Where no policy is provided, it is to be handled in accordance with the requirements of this D&S.

C. Storage.

(1) CUI designated materials, including all portable media (such as removable drives, CDs/DVDs, USB drives, and other portable storage devices), will be stored in a building, room, area, or locked container that has sufficient physical access control measures in place to prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know. Physical access control measures, that provide adequate delay or detection of unauthorized attempts to gain access by an adversary, include one or more of the following: guards, locks, electronic access control systems, locked file cabinets, locked desk drawers, or similar locked compartments or spaces.

(2) Hard copy Privacy Act information, including personnel files, will be stored separately from other CUI materials, as well as other uncontrolled information, in

locked metal cabinets, or other similar storage containers following Privacy Act storage requirements.

(3) CUI will not be stored in the same container used for the storage of classified information unless there is a distinct correlation between the information. When CUI materials are stored in the same container used for the storage of classified materials, the CUI materials will be segregated from the classified materials to the extent possible, e.g., separate folders, separate drawers, unless such information is integral to the classified media or document.

(4) CUI stored in Government-controlled IT data networks, applications, or devices will have additional controls levied that restrict access to all files containing sensitive information. Reclamation will authorize CUI access on an individual basis and only after validation of both "need-to-know" and of active participation in a specific official Government task or project has been established. No one with access to CUI may store that information on a non-Government-controlled network or device.

(5) IT systems that store CUI will be assessed and accredited for operation in accordance with applicable Federal and Reclamation standards.

D. Transmission.

(1) Transmission of Hard Copy CUI within the U.S. and its Territories:

(a) At a minimum, material will be placed in a single envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office, and the name of the intended recipient, if known. No indication of the sensitivity of the contents will be shown on the outside of the envelope.

(b) CUI materials must be mailed by U.S. Postal Service First Class Mail with tracking capability or an accountable commercial delivery service. Packages shall be tracked by automated tracking and/or accountability tools.

(c) CUI materials entered into an inter-office mail system must be afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

(2) Transmission to International Offices. When an overseas office is serviced by a military postal facility, i.e., APO/FPO, CUI will be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be hand carried or forwarded through the Department of State, Diplomatic Courier Service.

(3) Electronic Transmission.

(d) Transmittal via Fax. All CUI transmitted by fax must be properly marked prior to transmission. If CUI is transmitted by fax machine, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure.

(e) Transmittal via E-mail. All CUI transmitted by email must be properly marked prior to transmission. CUI transmitted via e-mail within the Department's network is already encrypted and does not require additional encryption. CUI that is e-mailed to addresses outside the Department must be encrypted. CUI must NOT be sent or forwarded to personal e-mail accounts.

(f) Posting on Internet/Intranet. CUI will not be posted on any internet or intranet website. CUI posted on Reclamation servers, such as SharePoint or team drives, must have an additional user authentication or permission set to control access.

(g) Telephone. If CUI is discussed on a telephone or video, appropriate procedures must be taken to ensure the conversation is not overheard by someone without a demonstrated need-to-know. Where feasible, individuals must consider the use of secure communications when discussing CUI information.

E. Decontrol, Retention, and Disposal.

(1) CUI must be decontrolled as soon as practical, in accordance with all applicable decontrol markings. When information is decontrolled, the CUI markings will be lined through on the first page or cover sheet with a new electronic or hand-written marking indicating the information has been DECONTROLLED and by whom.

(2) Retention and disposal of CUI records material will be in accordance with Reclamation's Information Management Handbook, Volume II: Records Retention Schedules.

(3) When disposal of CUI by destruction is appropriate, it will be accomplished in the following manner:

(a) Printed paper materials (reports, drawings, photographs, typed or handwritten notes, etc.) will be destroyed by shredding, burning, pulping, or pulverizing to assure destruction beyond recognition and reconstruction. If material is shredded, at a minimum, a crosscut shredder must be used.

(b) CUI materials must only be disposed of via recycling if the recycling bin is locked, remains locked, and inaccessible to unauthorized exposure until the materials are destroyed by shredding, burning, pulping, or pulverizing. Recycling contractors must validate that recycling containers remain locked until the materials are destroyed.

(c) Electronic storage media (disks/CDs/DVDs/tapes) and hard drives from copiers, scanners, and other electronic devices used to process or transmit CUI must be sanitized prior to disposal, in accordance with Reclamation Manual D&S, Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal – Information Sanitization (RM 08-13).

F. Incident Reporting.

(1) Loss, compromise, suspected compromise, or unauthorized disclosure of CUI will be reported immediately to your supervisor and a Reclamation security officer. IT incidents involving CUI will be reported to the Reclamation Enterprise Service Center (800-595-8344 or 303-445-3357, or email ITSecurityIncidents@usbr.gov) in accordance with Reclamation's IT incident reporting requirements (see the Reclamation Incident Response Standard Operating Procedures).

(2) Suspicious or inappropriate requests for information by any means shall be coordinated with a Reclamation security officer for risk evaluation and the validity of the request.

(3) When circumstances warrant, an inquiry will be conducted by a Reclamation security officer, the Computer Security Incident Response Team, or other designee to determine the cause and effect of the incident.

7. Related D&S.

For related and supporting Reclamation Manual D&S, see: Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal (IRM 08-13); Records and Information Management (RCD 05-01).

8. Definitions

A. Access.

Opportunity and ability to use or gain knowledge of information, records, or data as required in the performance of specific official government business.

B. Authorized Holder or Holder.

Reclamation employee, contractor, or consultant who has access to and maintains CUI in performance of their official duties.

C. CUI.

The official term used within the Executive Branch to identify sensitive information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

D. Information.

Facts, data, and knowledge created, received, and maintained for use by Reclamation to document its program decisions and mission-related activities, regardless of type, storage media, or format.

E. Need-to-Know.

The determination made by an authorized holder (see Paragraph 7.B.) of sensitive information that a prospective recipient requires access to the information in order to perform or assist in a lawful and specified authorized governmental function, i.e., access is required for the performance of specific official duties.

F. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards.

Comprehensive set of reliability standards and requirements established by NERC to ensure the security of electronic communications and control systems needed to plan, reliably operate, and support the North American bulk power system.