Reclamation Manual

Directives and Standards

Subject: Identifying and Safeguarding For Official Use Only (FOUO) Information

Purpose: Describes the requirements and procedures for identification and safeguarding sensitive but unclassified information referred to herein as FOUO information. 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); Executive Orders (EO) 10450, 10577, 12968, and 13526; Homeland Security Presidential Directives; Federal Information Processing Standards 200 and 201; and Departmental Manual (DM) Parts 380, 442, 444 and 446.

Approving Official: Director, Security, Safety, and Law Enforcement (SSLE)

Contact: SSLE, Security Office (84-450000)

1. **Introduction.** This D&S provides the minimum requirements for safeguarding all FOUO information, including draft information, originated within Reclamation. This also applies to all FOUO information received by Reclamation from non-Reclamation entities, where those entities do not provide specific safeguarding guidance.

2. **Applicability.**

   A. This D&S is applicable to all Reclamation offices, employees, contractors, and consultants.

   B. This D&S does not apply to classified national security information, which is covered by EO 12958, as amended.

3. **Definitions.**

   A. **Access.** One's ability to use, or opportunity to gain knowledge of, information, records, or data as required in the performance of official government business.

B. **Authorized Holder or Holder**. Reclamation employee, contractor, or consultant who has access to and maintains FOUO information in performance of their official duties.

C. **North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards.** Comprehensive set of CIP reliability standards and requirements established by NERC to ensure the security of electronic communications and control systems needed to plan and reliably operate and support the North American bulk power system.

D. **FOUO.** The official term used within Reclamation to identify unclassified information of a sensitive nature the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Note: FOUO information does not include information that is classified Confidential, Secret, or Top Secret under EO 13526, *Classified National Security Information* or its predecessor or successor orders.

E. **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.

F. **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 authorized governmental function, i.e., access is required for the performance of official duties.

4. **Responsibilities.**

A. **Director, SSLE.** The Director, SSLE, working through the Chief Security Officer, is responsible for:

(1) overseeing program activities to identify and safeguard FOUO information;

(2) promulgating Reclamation FOUO policy, D&S, and guidance as applicable; and

(3) developing and delivering necessary training materials and forums to educate employees and others on the proper recognition and safeguarding of FOUO information.

B. **Associate Chief Information Officer (ACIO).** The ACIO is responsible for:

(1) managing all records including compliance procedures, appraisal, and retention and disposal schedules;

(2) ensuring the security of Reclamation information technology (IT) systems and the information contained within those systems;

(3) developing and delivering necessary training materials and forums to educate employees on the safeguarding of FOUO information and records substantially addressing IT systems or information held within IT systems; and

(4) managing of Reclamation's Freedom of Information Act (FOIA) program.

C. **Directors, Managers, and Supervisors.** Directors, managers, and supervisors are responsible for:

(1) ensuring compliance with the standards for safeguarding FOUO and Highly Sensitive FOUO information as cited in this D&S;

(2) ensuring adequate procedures, education, and awareness are established and maintained, with emphasis on safeguarding of FOUO and Highly Sensitive FOUO information and prevention of unauthorized disclosure; and

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

D. **Regional Security Officer.** The regional security officers are responsible for regional implementation of this D&S, employee awareness, oversight, and serving as a technical link for the regional and area offices regarding this D&S.

E. **Regional IT Security Manager.** The regional IT security managers are responsible for the security of regional IT systems and the information contained within those systems

F. **Employees, Contractors, Consultants.** Reclamation employees, contractors, consultants, and others that generate or have access to FOUO information are responsible for:

(1) Being aware of and complying with the safeguarding requirements for FOUO and Highly Sensitive FOUO information as outlined in this D&S.

(2) Being aware that divulging information without authority could result in administrative or disciplinary action.

(3) Informing their supervisor and a security officer of any procedures or incidents that could result in the inappropriate disclosure or compromise of FOUO information.

(4) Identifying and marking information that is FOUO. Recipients or holders of unmarked Reclamation information who conclude the specific information is to be marked as FOUO will protect the 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 FOUO information.

5. **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 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.**

(1) The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

(2) Information is designated as sensitive in order to protect, control, and restrict access, as permissible under laws and regulations. The release of such information could 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. There are various categories of sensitive information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury Information, etc. In addition, there are numerous additional designations employed by various agencies to identify unclassified information as sensitive, e.g., FOUO, Law Enforcement Sensitive, Official Use Only, Limited Official Use, etc. Regardless of the designation used to identify it, the reason for the designation does not change. The use of these and other categories will be governed by the statutes and regulations issued for the applicable category of information, as well as this D&S.

C. **FOUO Designation.** Within Reclamation, the designation FOUO will be used to identify sensitive but unclassified information that is not otherwise specifically designated and marked in accordance with other statutes or regulations.

D. **FOIA Disclosure.** Information designated as FOUO 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.

E. **Inappropriate Use of the FOUO Designation.** Designation of information as FOUO 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.

F. **Designation Responsibility.** Any Reclamation employee, detailee, or contractor has the responsibility to designate sensitive information as FOUO and require any parties outside Reclamation to protect it under FOUO requirements.

G. **Duration of Designation.** Information designated as FOUO 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. [Reference Reclamation Manual D&S, *Managing Information, Records and Data Designated FOR OFFICIAL USE ONLY (FOUO)* (IRM 02-02) Paragraph 5.C.]

H. **Other Agency Information.** When receiving FOUO equivalent information from another government agency, it must be handled in accordance with the requirements provided by the other submitting governmental agency. Where no requirements are provided, it is to be handled in accordance with the requirements of this D&S.

I. **Visual Identity (VI).** In most instances, FOUO information is not intended for public release. Nevertheless, it is intended that, where applicable, FOUO information also comply with Reclamation's VI requirements (see Reclamation Manual Policy, *Visual Identity* (ADM P05), associated D&S, and Reclamation's VI Intranet site).

6. **FOUO Information.**

A. **General Types of FOUO Information.** The following types of information will be designated and safeguarded as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statute or regulation will take precedence. For example, if information meets the standards for designation as Law Enforcement Sensitive Information, then Law Enforcement Sensitive requirements for marking, handling, and safeguarding will take precedence. FOUO information includes, but is not limited to:

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

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

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

(4) Information that could result in increased harm to personnel, facilities, property, or the public.

(5) Internal IT systems data revealing information about the configurations of servers, desktops, applications, and networks, including: names, versions, and patch levels of applications; configurations and topologies of network switches, routers, firewalls, and gateways; significant network interconnections; carriers and locations of significant communications centers; deployment of intrusion detection and prevention tools; access and authentication methods; and significance of mission or business use/need. Examples of IT FOUO information are systems vulnerability scan results and firewall rule-sets. For further information contact the Bureau IT Security Manager. Information pertaining to national security systems eligible for classification under EO 12958, as amended, will be classified as appropriate.

(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 such as might be associated with a Reclamation IT system.

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

(8) Information that could constitute an indicator of U.S. Government intentions, capabilities, operations, activities, or otherwise threaten operations.

(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. **Highly-Sensitive FOUO Information.** Highly-Sensitive FOUO information is information which requires a greater degree of control and restricted access. Such information warrants additional protective handling measures beyond the minimum established requirements. For example, certain types of security vulnerabilities that could impact Reclamation operations may be considered "Highly Sensitive" based on the associated consequences if such sensitive information is compromised. Additional security controls for Highly-Sensitive FOUO information are found in Paragraph 7.G.

C. **Specific Examples of Reclamation FOUO Information.** Examples of Reclamation FOUO and Highly-Sensitive FOUO information 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.

7. **General Required Handling Procedures.** FOUO and Highly-Sensitive FOUO handling procedures are also summarized on the reverse side of the FOUO cover sheet (Appendix B). Additional requirements for Highly-Sensitive FOUO Information can be found in Paragraph 7.G.

A. **Marking.**

(1) Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and safeguarding requirements. The lack of FOUO markings does not relieve a holder from safeguarding responsibilities. All holders will protect FOUO accordingly, even that information which is not properly marked. Other sensitive information protected by statute or regulation will be marked in accordance with the applicable procedures for that type of information and need not be additionally marked FOUO.

(2) These marking procedures will apply to all newly-developed FOUO information, or when existing information is distributed or disseminated. Existing information that is considered FOUO information or that which has been previously marked as protected information under any previous Reclamation direction does not require new marking or revised marking until the specific information is handled or released. All FOUO information will be stored in accordance with this D&S.

(a) Prominently mark the center top and bottom of the front cover, first page, title page, and each individual page containing FOUO information with "FOR OFFICIAL USE ONLY" in capital letters. (See Appendix D.)

(b) FOUO information being transmitted to recipients outside of Reclamation that have a "need-to-know," (e.g., other Federal agencies; state or local emergency response officials, etc.) must include the following additional notice placed prominently on the first page and/or cover sheet.

> **WARNING:** This information is **FOR OFFICIAL USE ONLY** and must be protected. This US Government data may be exempt from further public release under the Freedom of Information Act (5 U.S.C. 552). This information must be controlled in accordance with applicable Bureau of Reclamation directives. The further distribution of this information requires prior approval from an authorized Reclamation official.

(c) Computer storage media, e.g., disks, tapes, CDs/DVDs, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY" or "FOUO" with permanent marker, label, or stamp.

(d) Individual portion or paragraph markings (i.e., markings normally used in classified documents) are not required on a document that contains only FOUO information. Designator or originator information and markings, downgrading instructions, and date/event markings are optional but not required.

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked in accordance with the applicable classification guide.

B. **Dissemination and Access.**

(1) Access to FOUO information is based on need-to-know 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. FOUO information may be shared with contractors; operating entities; other agencies; Federal, state, tribal, or local government; and emergency and law enforcement officials provided the information is shared in furtherance of a coordinated and official governmental activity.

(2) FOUO information will not be disseminated in any manner – orally, visually, or electronically – to individuals or organizations not performing or assisting in a lawful and authorized government function and not demonstrating appropriate need-to-know. However, 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.

(3) The holder of the protected information will comply with any access, protective handling, dissemination, and destruction restrictions.

(4) A security clearance or background investigation is not required for need-to-know access to FOUO information.

(5) When discussing or transferring FOUO information to another individual, the holder must ensure precautions are taken to prevent unauthorized compromise of the protected information.

(6) All FOUO documents shared with outside entities or individuals will include the warning statement discussed in Paragraph 7.A.(2). A non-disclosure agreement (Appendix E) is optional, but not required prior to the dissemination of the information.

(7) Other sensitive information protected by statute or regulation, e.g., Privacy Act, will be controlled and disseminated in accordance with the applicable requirements for that type of information.

(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) FOUO designated materials 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. Sufficient access control must be provided by guards, locks, card readers, locked file cabinets, locked desk drawers, or similar locked compartments or spaces.

(2) FOUO information 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 FOUO materials are stored in the same container used for the storage of classified materials, the FOUO materials will be segregated from the classified materials to the extent possible, e.g., separate folders, separate drawers, etc.

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

(4) The portable media that is used to store FOUO information, such as laptop computers, removable drives, CDs/DVDs, USB drives, and other portable storage devices, must be stored, marked, and protected to the same level as the information stored to provide identification and prevent loss, theft, unauthorized access, and unauthorized disclosure.

D. **Transmission.**

(1) **Transmission of Hard Copy FOUO 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) FOUO materials must be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service.

(c) FOUO 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, FOUO 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.**

(a) **Transmittal via Fax.** If FOUO information is transmitted by fax machine, preferably secured, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure. (See Appendix C for sample FOUO fax cover sheet.)

(b) **Transmittal via E-mail.** FOUO information transmitted via e-mail without encryption must only occur within the Department's network. FOUO information that is e-mailed to addresses outside the Department must be encrypted. FOUO information is NOT to be sent or forwarded to personal e-mail accounts.

(c) **Posting on Internet/Intranet.** FOUO information will not be posted on any Internet (public) Web site. FOUO information posted on the Reclamation Intranet or other government controlled or sponsored data networks, including SharePoint sites, must have password authentication protection or user access control.

(d) **Telephone.** FOUO information may be discussed on a telephone; however, appropriate procedures must be taken to ensure that the conversation is not overheard by someone without a demonstrated need-to-know.

E. **Retention and Disposal.**

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

(2) When disposal of FOUO information 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) FOUO materials must only be disposed of via recycling if the recycling bin is locked, and remains locked, 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) will be sanitized by degaussing, wiping, erasing, or physical destruction. Contact your local IT security personnel or regional IT security manager for additional information.

F. **Incident Reporting.**

(1) The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported immediately to your supervisor and a Reclamation security officer. IT incidents involving FOUO information will be reported to the appropriate Computer Security Incident Response Center in accordance with Reclamation's IT incident reporting requirements (see the *Reclamation Computer Security Incident Response Handbook*).

(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 or by the Computer Security Incident Response Team or other designee to determine the cause and effect of the incident.

G. **Highly-Sensitive FOUO Information.** For this type of information, the following additional security controls will be implemented to afford a higher level of protection. The need for additional safeguarding will be determined by any Reclamation employee or contractor that believes additional protections are prudent and necessary. Highly-Sensitive FOUO information will:

(1) Be prominently marked at the center top and bottom of the front cover, first page, title page, and each individual page containing Highly-Sensitive FOUO information with "HIGHLY-SENSITIVE//FOR OFFICIAL USE ONLY." (See Appendix D.)

(2) Be identified, transmitted, and stored with an FOUO cover sheet. This cover sheet is shown in Appendix B and is available as Reclamation Form No. 7-2564.

(3) Be stored in a locked file cabinet, locked desk drawer, locked overhead storage compartment, or similar locked compartment—in addition to being inside a building, room, or area with access control measures (see Paragraph 7.C.). Where possible, Highly-Sensitive information must be locked in a safe or an accredited secure facility.

(4) Be stored on assessed and accredited IT systems in encrypted/password protected form.

(5) Be encrypted when transmitted by e-mail or on portable media. The password shall be transmitted in a separate e-mail or by telephone.

(6) Not be posted on the Internet or Intranet. Highly-Sensitive information posted on Reclamation SharePoint sites must be in encrypted form.

(7) Not be discussed while using wireless devices, unless in an emergency situation.

(8) Only be shared with individuals who have a demonstrated need-to-know.

(9) Only be shared with individuals outside of Reclamation who have signed a Non-Disclosure Agreement. This requirement may be waived for employees of other Federal agencies or our managing partners at the discretion of Reclamation's Chief Security Officer or regional security officer. (See Appendix E.)

(10) Not be disposed of in recycling receptacles, including locked bins as discussed in Paragraph 7.E., until the materials have first been destroyed as specified in Paragraphs 7.E.(2)(a) and (c).

H. **Other Protective Marking.** Where applicable to protect Law Enforcement Sensitive information, the following procedure will be used. Prominently mark at the center top and bottom of the front cover, first page, title page, and each individual page containing Law Enforcement Sensitive information with "LAW ENFORCEMENT SENSITIVE//FOR OFFICIAL USE ONLY." (See Appendix D.)

8. **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); and *Managing Information, Records, and Data Designated FOR OFFICIAL USE ONLY (FOUO)* (IRM 02-02).

RECLAMATION
Managing Water in the West

RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: **06/13/2016** Release No. **512**

Ensure all employees needing this information are provided a copy of this release.

Reclamation Manual Release Number and Subject

SLE 02-01 Identifying and Safeguarding For Official Use Only (FOUO) Information

Summary of Changes

Minor revisions approved to reflect changes to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards. All references to requirements from previous versions of the standards were removed. Additional minor word changes were necessary to reflect the wording changes in the updated standards.

NOTE: This Reclamation Manual release applies to all Reclamation employees. When an exclusive bargaining unit exists, changes to this release may be subject to the provisions of collective bargaining agreements.

Filing instructions

Remove Sheets	Insert Sheets
SLE 02-01 pp 1-14	**SLE 02-01 pp 1-14**
Appendix A pp 1-3	**Appendix A pp 1-3**
Appendix B pp 1-2	**Appendix B pp 1-2**
Appendix C p 1	**Appendix C p 1**
Appendix D p 1	**Appendix D p 1**
Appendix E p 1	**Appendix E p 1**

All Reclamation Manual releases are available at http://www.usbr.gov/recman/

Filed by: _____ Date: _____