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 of sensitive but unclassified information referred to herein as FOUO information. The benefits of this Directive and Standard are to provide standard instructions on sensitive but unclassified information. In addition, this Directive and Standard helps to align Reclamation with other governmental practices regarding protection of this type of information.

Authority: Office of Management and Budget (OMB) Circular A-130, Appendix III; OMB Circular A-123, Internal Control Systems, Critical Infrastructure Assurance Office Practices for Securing Critical Information Assets (January 2000); Department of the Interior Departmental Manual Part 375 Chapter 19; Executive Order (EO) 12958, as amended; EO 12968; EO 13292; Safety of Dams Act of 1978; Federal Records Act – U.S.C. Title 44, Chapters 21, 29, 31, 33; Paperwork Reduction Act – U.S.C. Title 44, Chapter 35; 36 CFR Subchapter B, Part 1220-1238; Departmental Manual 380 DM 1, 2, 3, and 6.

Approving Official: Director, Security, Safety, and Law Enforcement

Contact: Security, Safety, and Law Enforcement Office, Security Office, 84-45000

1. **Scope.**

   A. This Directive and Standard 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. To enhance the exchange of FOUO information with other Federal agencies, this Directive and Standard is partially based on the Department of Homeland Security directive entitled "Safeguarding Sensitive but Unclassified (FOR OFFICIAL USE ONLY) Information." This Directive and Standard does not apply to national security information, which is covered by EO 12958, as amended.

   B. This Directive and Standard supersedes interim Reclamation policy found in the Commissioner's memorandum dated June 19, 2002, entitled "Policy Memorandum – Interim Requirements and Procedures for Handling and Safeguarding the Bureau of Reclamation's Information and Records." This Directive and Standard also supersedes Reclamation Manual Directive and Standard, *Reclamation Information Technology (IT) Security Program: Information/Data Security* (IRM 08-11). Under this Directive and Standard, Reclamation will no longer separate FOUO information into distinct

"Restricted" and "Sensitive" categories, as was directed under the previous policy and memorandum.

2. **Applicability.** This Directive and Standard is applicable to all Reclamation offices, employees, contractors, consultants, and others.

3. **Definitions.**

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

   B. **For Official Use Only.** The official term used within Reclamation to identify unclassified information of a sensitive nature, not otherwise protected by statute or regulation, 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. Information impacting the national security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, *Classified National Security Information*, as amended, or its predecessor or successor orders, is NOT to be considered FOUO. FOUO information is not to be considered classified.

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

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

4. **Responsibilities.**

   A. **Director, Security, Safety, and Law Enforcement (SSLE).** The Director, SSLE, working through the Chief Security Officer, is responsible for:

      (1) Oversight of program activities to identify and safeguard FOUO information.

      (2) Promulgation of Reclamation FOUO policy, directives and standards, and guidance as applicable.

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

B. **Chief Information Officer.** The Chief Information Officer is responsible for:

(1) All records management responsibilities including compliance procedures, appraisal, and retention and disposal schedules.

(2) The application of this Directive and Standard to information held within or substantially addressing IT systems.

(3) Development and delivery of 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.

C. **Directors, Managers, and Supervisors.** Heads of Reclamation offices and organizational elements are responsible for:

(1) Ensuring compliance with the standards for safeguarding FOUO information as cited in this Directive and Standard.

(2) Ensuring adequate procedures, education, and awareness are established and maintained, with emphasis on safeguarding of FOUO information and prevention of unauthorized disclosure.

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

D. **Regional Security Officer.** The Regional Security Officers are responsible for regional implementation of this Directive and Standard, employee awareness, oversight, and serve as a technical link for the regional and area offices regarding this Directive and Standard.

E. **Regional IT Security Manager.** The Regional IT Security Managers are responsible for regional application of this Directive and Standard to information held within or substantially addressing IT systems.

F. **Employees and Others.** 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 information as outlined in this Directive and Standard.

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

(3) Informing their supervisor and appropriate 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 should be FOUO. Recipients or holders of unmarked Reclamation information who conclude that the specific information should be marked as FOUO will protect the information and promptly notify the originator of their determination.

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 Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Contact your local Records or FOIA Officer for additional identification and handling guidance for Federal records.

B. **Sensitive Information.** 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." However, information otherwise protected by EO or act of Congress can also be considered FOUO for the purposes of greater protection.

(1) Specific standard criteria and terminology defining the types of information warranting designation as "sensitive" does not exist within the Federal government, with the exception of certain types of information protected by statute. Such designations are left to the discretion of each individual agency.

(2) Information is designated as sensitive in order to protect, control and restrict access. 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 interests. Within "sensitive but unclassified," there are various categories of 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 Directive and Standard.

C. **FOUO Designation.** Within Reclamation, the designation "For Official Use Only" will be used to identify sensitive but unclassified information that is not otherwise specifically described and governed by other statute or regulation (see Paragraph 5.B.(2)).

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 Authority.** Any Reclamation employee, detailee, or contractor has the authority and responsibility to designate information as FOUO.

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 Directive and Standard, *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 is to be handled in accordance with the guidance provided by the other submitting governmental agency. Where no guidance is provided, it is to be handled in accordance with the requirements of this Directive and Standard.

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 Visual Identity guidelines.

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 statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Law Enforcement Sensitive Information, then Law Enforcement Sensitive guidance for marking, handling, and safeguarding will take precedence. For purposes of this Directive and Standard, FOUO information is:

(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 be sold for profit.

(5) Information that could result in risk to personnel or property.

(6) 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 guidance contact the Bureau Information Technology Security Manager. Information pertaining to national security systems eligible for classification under EO 12958, as amended, will be classified as appropriate.

(7) Security data revealing 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 certification and accreditation documentation such as might be associated with a Reclamation IT system.

(8) Reviews or reports illustrating or disclosing asset infrastructure or security vulnerabilities of persons, systems, or facilities, not otherwise eligible for classification under EO 12958, as amended.

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

(10) 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.

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

(12) Certain research and development information where such information may reveal vulnerabilities, result in risk to personnel or property, or constitute the intellectual property of a non-Federal entity or individual.

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 should such sensitive information be compromised. Additional security controls for Highly Sensitive FOUO information are found in Paragraph 7.G.

C. **Examples of Reclamation FOUO Information.** Examples of Reclamation FOUO information are given in Appendix A. Appendix A only provides examples and is not intended to serve as an all-inclusive list.

7. **General Required Handling Procedures.** FOUO handling procedures are also summarized on the reverse side of the FOUO cover sheet (Appendix B).

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 guidance 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 would be considered to be 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 Directive and Standard.

(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) E-mails and materials being transmitted to recipients outside of Reclamation that have a "need-to-know," (e.g., other federal agencies, state, local officials, other entities, 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 also not required, but are optional.

(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, among others, 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.

(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 that the individual with whom the discussion is to be held or the information is to be transferred to has a valid need-to-know. In addition, the holder must ensure that 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).

(7) Other sensitive information protected by statute or regulation, e.g., Privacy Act, will be controlled and disseminated in accordance with the applicable guidance 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 guidance is provided, it is to be handled in accordance with the requirements of this Directive and Standard.

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 may 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, they 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 certified 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 opaque 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 may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service.

(c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed opaque envelope.

(2) **Transmission to Overseas 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.** FOUO information may be transmitted by fax machine. Where available, the use of a secure fax machine is encouraged. 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 may be transmitted via e-mail without encryption. 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) website. However, FOUO information may be posted on the Reclamation intranet or other government controlled or sponsored data networks with password authentication protection.

(d) **Telephone.** FOUO information may be discussed on a telephone.

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) Photographs, typed or handwritten notes and printed paper materials will be destroyed by shredding, burning, pulping, or pulverizing, such as to assure destruction beyond recognition and reconstruction. If material is shredded, at a minimum, a crosscut shredder must be used.

(b) FOUO materials may be disposed of via recycling only 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 guidance.

F. **Incident Reporting.**

(1) The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported immediately to the appropriate 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 (reference the *Reclamation Computer Security Incident Response Handbook*).

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

(3) Additional notifications to management will be made without delay when the disclosure or compromise could result in physical harm to an individual or the compromise of a planned or ongoing operation.

(4) When circumstances warrant, an inquiry will be conducted by the appropriate 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 may 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 available, Highly Sensitive information should be locked in a safe or an accredited secure facility.

(4) Be stored on certified and accredited IT systems in encrypted form. The encryption employed must meet the requirements of Federal Information Processing Standard (FIPS) 140-2, and be validated to at least level 1.

(5) Be encrypted when transmitted by email. Use of Federal Information Processing Standard approved encryption software is required.

(6) Not be posted on the Internet or intranet.

(7) Not be discussed over telephones except under emergency conditions.

(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 Directives and Standards.** For related and supporting Reclamation Manual Directives and Standards, see: IRM 08-13, *Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal;* RCD 05-01, *Records and Information Management;* and IRM 02-02, *Managing Information, Records, and Data Designated FOR OFFICIAL USE ONLY (FOUO).*