Reclamation Manual

Directives and Standards

Subject: Personnel Security and Suitability

Purpose: To describe the purpose, responsibilities, requirements, and procedures of the Bureau of Reclamation's Personnel Security and Suitability Program (PSSP). The benefits of this Directive and Standard (D&S) are establishment of consistent personnel security and suitability requirements and procedures.

Authority: Computer Security Act of 1987 (Pub. L. 100-235); Chapter 3 and 73 of Title 5, United States Code (USC), *Government Organizations and Employees*; 5 Code of Federal Regulations (CFR) 731, *Suitability;* 732, *National Security Positions;* and 736, *Personnel Investigations*; Executive Orders (EOs) 10450, *Security Requirements for Government Employment*, 10577, *Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service*, 12958, *Classified National Security Information*, 12968, *Access to Classified Information*, and 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, as amended; Appendix III to Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*; Federal Information Processing Standards (FIPS) Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*; and Departmental Manual (DM) Parts 441, *Personnel Security and Suitability Requirements*, 442, *Classified National Security Information*, 443, *Industrial Security Program*, 444, *Physical Protection and Facility Security*, and 446, *Law Enforcement*.

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

Contact: SSLE Office, 84-450000

1. **Introduction.**

   A. The Federal government mandates by law, EO, Presidential Directives, regulations, and guidance that employment and work assignments for all applicants, appointees, Federal employees, contractors, and others are consistent with national security and suitability guidelines. The PSSP has four main purposes: (1) to provide a basis for determining a person's suitability for assignment to Federal work and/or Federal employment, (2) to provide a basis for Reclamation to determine whether a Federal employee should be

granted a national security clearance, (3) to implement certain Personal Identity Verification (PIV) requirements of HSPD-12, and (4) general risk management of potential insider threats.

B. This D&S establishes procedures which supplement and clarify the requirements and procedures for Reclamation in determining personnel security and suitability matters contained in DM Parts 441, 442, 443, 444, and 446; 5 CFR Parts 731, 732, and 736; and 5 USC Chapters 3 and 73.

2. **Applicability.** This D&S applies to all Reclamation applicants, appointees, and Federal employees, plus contractors, volunteers, and other individuals that are required to have a background investigation pursuant to the authorities listed above.

3. **Definitions.** The following terms are used within this D&S and may be unique to Reclamation. They are provided as a supplement to and clarification of terms defined or utilized in various applicable EO, DM, and/or CFR.

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

B. **Adjudicative Determination.** The analytical review of the results of a completed background investigation to determine if the individual's character and conduct promotes the efficiency of the Federal service and/or is in the interest of national security.

C. **Background Investigation.** A report of information of an individual's employment, criminal, and personal history to determine an individual's suitability, qualifications, and/or eligibility for access to classified information for applicants, appointees, Federal employees, contractors, volunteers, and other individuals.

D. **Classified Information.** Classified information, as defined by EO 12958, as amended, is information regardless of form that requires protection against unauthorized disclosure. Classified information is identified by the appropriate markings indicating the level of access (see also definition of "Sensitive" in Paragraph 3.R.).

E. **Derogatory Information.** Information that indicates an individual's employment, continuing employment, or assignment of work with the Federal government may not reasonably be expected to promote the efficiency of the Federal service or expected to be clearly consistent with the interests of national security.

F. **Efficiency of the Service.** The employer's verification that the applicant or employee is able to perform the duties and responsibilities of the position while protecting the

integrity of the Federal service, and his/her presence on the job or conduct (on or off duty) will not inhibit other employees or the agency from performing their functions.

G. **Fingerprint Transmission System.** System in which electronic fingerprints captured at an HSPD-12 Credentialing Center are electronically transmitted to the Office of Personnel Management (OPM) and is used to expedite the background investigation process, eliminate the manual paper process, improve quality control, and provide end-to-end accountability.

H. **Foreign National.** A person visiting or residing in the United States (U.S.) who is a citizen of any country other than the U.S. This includes legal permanent residents otherwise known as permanent resident aliens.

I. **Interim Security Clearance.** A certification based on partial investigative action that a U.S. citizen, who requires immediate access to classified information, has been found eligible for and granted temporary (pending a completed favorably adjudicated background investigation) access to classified information at a specified level (e.g., up to the Secret level) under Federal standards.

J. **Law Enforcement Officer.** A sworn and commissioned officer to enforce criminal statutes and authorized to carry firearms, execute and serve warrants, search, seize, make arrests, and perform such duties as authorized by law.

K. **National Security Clearance.** An administrative determination and authorization, granted in writing based upon the results of an investigation that an individual is trustworthy and may be granted eligibility for access to classified information to the level required in the performance of assigned duties in a position designated as a national security position. Also referred to as Security Clearance. Note: A favorably adjudicated background investigation, by itself, does not convey a Security Clearance.

L. **National Security Position.** Positions designated as “sensitive” at specific national security sensitivity levels, incumbents of which are eligible for access to classified information associated with each particular level. Any position in which the employee could bring about, because of the nature of the position, a material adverse effect on the national security. There are three types of national security positions, which require access to classified information:

(1) **Special Sensitive Position.** Any position, the duties of which are determined to be at a level higher than "critical sensitive" because of a greater degree of damage that an individual occupying the position could do to the national security, or because the duties may entail access to Sensitive Compartmented Information (SCI).

(2) **Critical Sensitive Position.** Any position with a requirement for access to Top Secret information.

(3) **Non-Critical Sensitive Position.** Any other national security position that does not fall within the definition of a critical or special sensitive position. The duties of a non-critical sensitive position include, but are not limited to, access to national security information and material up to, and including, Secret.

M. **Need to Know.** The determination made by an authorized holder 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, i.e., access is required for the performance of official duties.

N. **Non-Sensitive/Low Risk Position.** Any position in Reclamation that does not fall within the definition of national security or public trust positions.

O. **Public Trust Position.** A high or moderate risk position that is not a national security position, meaning it does not require access to classified information, but may require access to sensitive but unclassified information. Public trust positions are designated at a specific level of risk based on the degree of damage that an individual, by virtue of the occupancy of the position, could do to the public or the Federal service.

P. **Reclamation Security Office.** The office within Reclamation's SSLE directorate where the management of Reclamation-wide security functions (including information, personnel, and facility security) resides. This does not include management of Information Technology (IT) or communications security which is part of the Information Resources Office.

Q. **Security Briefing Officer.** Any authorized official who has a national security clearance and may provide and explain the "Classified Non-Disclosure Agreement" form (SF 312) and process. This individual also witnesses the execution of the SF 312.

R. **Sensitive.** With regard to personnel security, "sensitive" position is a specific term that refers to a national security position (e.g., non-critical sensitive, critical sensitive, or special sensitive) requiring access to classified information.

S. **Suitability.** An individual's character, reputation, trustworthiness, and fitness for overall employment as related to the efficiency of the Federal service. This is the basic standard (within EO 10450, as amended,) requiring that an individual's appointment to (or retention in) the Federal service must promote the efficiency of the service.

T. **Suitability Pre-Screening.** The process of conducting an initial suitability review of an applicant or prospective candidate by a servicing Human Resources (HR) office staffing official for entrance into the Federal service or entrance into a higher level

public trust or national security position. This is only performed for suitability purposes based upon the suitability criteria contained within 441 DM 5 and 5 CFR 731 (see Paragraph 4.F.(5)).

U. **U. S. Citizen.** An individual born in one of the 50 United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or United States holdings in the Mariana Islands, the U.S. Virgin Islands, or the Panama Canal Zone (if the father and/or mother is/was a U.S. citizen). Also qualifying is a documented "naturalized" U.S. citizen.

4. **Responsibilities.** (Note: More detailed information is available in 441 DM 2).

A. **Reclamation Security Office.** Reclamation's Chief Security Officer (CSO), as the senior Reclamation security official, has overall responsibility for Reclamation's PSSP and the SSLE Personnel Security Office. This includes background investigation and adjudication of all public trust and national security positions, policy development, program oversight, and the security clearance briefing, granting, verification, and debriefing processes. Specific personnel security responsibilities of the CSO include, but are not limited to, the following:

(1) processing and adjudicating background investigations for all public trust and national security positions for Federal employees and contractor positions that are equivalent in risk level to Federal public trust positions;

(2) processing and adjudicating all low-risk positions for Denver and Washington Office Reclamation employees, and all contractor staff that are required to have a Federal PIV Card;

(3) conducting national security briefings, debriefings, and granting/verification of clearances;

(4) providing guidance and training to human resources specialists, managers, and employees throughout Reclamation on matters pertaining to background investigation processing and suitability adjudication;

(5) processing of background investigation waiver of pre-appointment investigative requirement (waiver) requests by validating eligibility and processing for approval;

(6) ensuring compliance with all investigative requirements; and

(7) maintaining records.

B. **Regional Directors.** Regional directors are responsible for designating the individuals and/or offices responsible for initiating and adjudicating background investigations associated with non-sensitive/low risk positions within their respective region, in accordance with this D&S (see Paragraph 8.F.).

C. **Regional Security Officers.** Regional security officers are responsible for:

(1) providing guidance to supervisors and managers on position risk/sensitivity designation (including contract positions); and

(2) conducting or witnessing SF 312 security briefings and debriefings.

D. **IT Risk and Portfolio Management Division.** The IT Risk and Portfolio Management Division, in collaboration with HR, is responsible for establishing minimum position designations for specific Reclamation IT positions (see Appendix A, Table 2).

E. **Denver HR Policy and Programs Division.** The HR Policy and Programs Division is responsible for ensuring consistency/oversight of servicing HR offices' implementation of position designations and related database and information reporting activities.

F. **Servicing HR Offices, or Other Designated Offices.** The servicing HR offices, or other office(s) as designated by the regional director, are responsible for:

(1) ensuring that the risk/sensitivity level of all Reclamation positions are designated in accordance with the OPM Position Designation Tool (PDT) and appropriate background investigations are initiated and conducted for all positions;

(2) communicating with employees during the adjudication process, including delivery of correspondence regarding requests for additional information and proposed and final suitability and national security determinations;

(3) keeping supervisors informed of potential adjudicative issues and implementing final personnel actions related to position designation, suitability, and national security.

(4) maintaining position designation information, in coordination with the hiring official, for all Reclamation Federal employee positions;

(5) performing initial suitability pre-screening of Reclamation Federal employees and applicants when there is a change in assignment (new hires, transferees, details, reassignments, temporary or permanent promotions, etc.) or a change in position risk or sensitivity level;

(6) processing and adjudicating background investigations of low-risk non-sensitive positions for Reclamation employees and any other individuals (e.g., contract employees) where a director has assigned HR this responsibility;

(7) ensuring processing and compliance with all waiver requirements for critical sensitive positions or Law Enforcement (LE) positions when applicable;

(8) reporting to the SSLE Personnel Security Office any information concerning significant employee issues (e.g., questionable conduct, financial misrepresentation, lack of trustworthiness, adverse actions, etc.) that may warrant a follow-up adjudication to determine whether the individual continues to be suitable for the position; and

(9) record-keeping and related database and information reporting including immediate notification to the SSLE Personnel Security Office of individuals in national security and public trust positions who are (or will be) separating from Reclamation's employment or their position is being re-designated.

G. **Managers and Supervisors.** Managers and supervisors are responsible for:

(1) ensuring that all positions under their authority have accurate Position Descriptions (PD) with accurate designation in terms of position risk/sensitivity levels;

(2) ensuring timely compliance of employees with all investigation and reinvestigation requirements, including completion of background investigation forms and responses to requests for additional information during the background investigation and adjudication process;

(3) ensuring timely compliance with all waiver requirements for critical sensitive positions or LE positions when applicable;

(4) reporting to the CSO or SSLE Personnel Security Office any information (i.e., personal conduct, criminal conduct, financial difficulties, delinquent taxes, etc.) that may indicate an individual's eligibility for access to classified information that appears to be inconsistent with the interests of national security; and

(5) reporting to the SSLE Personnel Security Office any information (i.e., personal conduct, criminal conduct, financial difficulties, delinquent taxes, etc.) that may indicate an individual does not continue to be suitable for the position. For low risk non-sensitive positions, information should be reported to the servicing personnel office or regional security office.

H. **Acquisition Management Offices (AMO) and Contracting Officer Representatives (COR).** The AMO and COR are responsible for: (see Department of the Interior (DOI) Acquisition Policy Release (DIAPR) 2010-04)

(1) ensuring that all contracts under their authority include required Reclamation Acquisition Regulation security clauses (see RAR Subpart 1437.81, *Security Requirements*);

(2) assisting in the PIV process by initiating the DOI Access card request in the DOI Access card system and ensuring contractor credentials are renewed and rescinded in a timely manner in the case of a change in contractor personnel, termination of a contract, etc.

(3) ensuring compliance with all investigation and reinvestigation requirements for contractor staff by verifying the required background investigation forms have been completed in a timely manner and with the background investigation process by providing the position sensitivity designations for contractor staff;

(4) as prescribed by the contract, taking action as a result of an adverse suitability determination of contractor staff (see Paragraph 8.G.(13)); and

(5) coordinating with contracting officers on the mandatory utilization of the requirements of the National Industrial Security Program (NISP) for any national security contracts as specified within 443 DM 1 (see Paragraph 9.E.).

I. **Reclamation Employees and Contractor Staff.** All Reclamation employees and contractor staff are responsible for:

(1) completing background investigation forms and responding to any additional requests for information during the background investigation and adjudication processes, within the time frame established by the personnel security adjudicator;

(2) reporting to his/her supervisor or COR, any job activities that they believe could result in a change in their PD or their need for increased security access;

(3) reporting to the CSO or SSLE Personnel Security Office any information (i.e., personal conduct, criminal conduct, financial difficulties, delinquent taxes, etc.) that raises potential security concerns about an individual with a national security clearance (including themselves) (see the U.S. Department of Defense (DOD) link at http://www.dhra.mil/perserec/osg/home.htm for more specific guidance on reporting requirements and also Paragraph 9.F.(2));

(4) reporting to the SSLE Personnel Security Office any information (i.e., personal conduct, criminal conduct, financial difficulties, delinquent taxes, etc.) that may indicate an individual does not continue to be suitable for the position (including themselves). For low risk non-sensitive positions, information must be reported to the servicing HR office or regional security office.

(5) assisting with and cooperating fully in any communications and/or forms completion related to the personnel security and/or suitability process;

(6) for individuals holding a national security clearance reporting all foreign travel to the SSLE Personnel Security Office prior to departure, including both official and non-official travel (see Paragraph 9.I.); and

(7) complying with all applicable personnel security and suitability laws, EOs, regulations, requirements, and instructions.

5. **Program / Position Designation Process.**

A. **General.** All Reclamation positions must be designated at a suitability risk level and (when applicable) a national security sensitivity level based on the degree of damage that an individual, by virtue of the occupancy of the position, could cause to the efficiency of the Federal service or national security.

B. **Program Designation.** This is a designation that assigns the program impact and scope of operation on a Reclamation-wide basis. Departmental Manual Part 441 Chapter 3 requires a consistent program placement based on the mission of the agency not on the individual duties of the position. Program designation is identified by the Denver HR Policy and Programs Division in the position designation process when utilizing the OPM PDT. Reclamation must use multi-agency as the program designation for all Reclamation positions.

C. **Position Designation.** In accordance with OPM Federal Investigative Notice 10-06, the OPM PDT must be used to determine the position risk/sensitivity designation (i.e., the national security sensitivity and/or suitability risk levels of a position.) This tool must be used in conjunction with the duties of the position identified in the PD and in collaboration with the supervisor/manager of the position.

D. **Position Designation Levels.** Each Reclamation position will be designated and the position designation level recorded on a position sensitivity designation sheet (generated from the OPM PDT), a PD cover sheet (OF-8), and in the Federal Personnel Payroll System (FPPS) at one of the risk or sensitivity levels identified in Table 1. In order to obtain Reclamation-wide consistency, several key Reclamation positions were designated through the use of the OPM PDT and the minimum position/risk sensitivity

designation levels are identified in Appendix A (along with corresponding background investigation levels, security clearances, and pre-appointment background investigation waiver requirements).

6. **Background Investigations.**

A. **General.** Every Federal employee and contractor is subject to a background investigation upon appointment to the job and upon placement in a position with a higher risk or sensitivity level. Some position risk levels also require periodic reinvestigations. In addition, all positions are subject to re-evaluation if new adverse information is discovered that could affect the individual's suitability for employment or access to classified information.

(1) Every Reclamation appointment is subject to investigation. The investigation's scope is determined by the risk and sensitivity level of the position that was determined by the position designation process.

(2) Background investigations are conducted by OPM on behalf of Reclamation in accordance with 5 CFR 731.104 and HSPD-12 requirements.

(3) Information about OPM background investigations can be accessed at http://www.opm.gov/investigations/.

(4) Investigations must be initiated (submitted to OPM) no later than 14 calendar days after placement in the position, but preferably prior to appointment.

B. **Risk/Sensitivity Level Changes.**

(1) If an individual will be moving to a position with a higher risk/sensitivity level, an upgraded background investigation is required. An individual can be placed into the position while the background investigation is being conducted, unless the position is a critical sensitive or an LE position. All critical sensitive or LE positions require an approved Waiver of Pre-Appointment Investigation Requirement (see Paragraph 6.H.) or a favorably adjudicated background investigation prior to placement into the position.

(2) If the risk/sensitivity level of the individual's current position changes to a higher level, an upgraded background investigation is required and the individual may encumber or remain in the position while the upgraded investigation is being conducted and adjudicated.

(3) Any upgraded investigation required for a new risk/sensitivity level must be initiated (submitted to OPM) within 14 calendar days of the effective date of the move or the new designation is finalized. Consequently, any request for an

upgraded investigation required for a new national security or public trust level must be transmitted to the SSLE Personnel Security Office prior to the effective date and as soon as possible.

C. **Types and Frequency of Investigations and Reinvestigations.** Table 1 gives the type of investigations and reinvestigations, and the frequency of reinvestigations that are required for each risk/sensitivity and security access level. Reinvestigations will be initiated 6 months prior to the applicable anniversary of their previous completion date (12 months for special sensitive positions). The period for calculating when a reinvestigation is to be initiated begins with the completion date (i.e., case closing transmittal date) of the prior investigation. For more specific information regarding the scope of each type of investigation, see 441 DM 4 tables on pages 7 through 9.

Table 1:

Position Risk Designation	National Security Access	Background Investigation	Minimum Background Reinvestigation	Frequency of Reinvestigation	FPPS Coding
Non-Sensitive/Low Risk[1]	None	Tier 1 (NACI)[2]	Not Applicable[1]	Not Applicable	1
PUBLIC TRUST POSITIONS:					
Non-Sensitive/ Moderate Risk	None	Tier 2S (MBI)[2]	Tier 2RS (NACLC)[2]	Every 5 years	5
Non-Sensitive/ High Risk	None	Tier 4 (BI)[2]	Tier 4R (PRI)[2]	Every 5 years	6
NATIONAL SECURITY POSITIONS:					
Non-Critical Sensitive/ Moderate Risk	Secret	Tier 3 (ANACI & PSI)[2]	Tier 3R (NACLC)[2]	Every 5 years	2
Non-Critical Sensitive/ High Risk	Secret	Tier 5 (SSBI)[2]	Tier 5R (SSBI-PR or PPR)[2]	Every 5 years	2
Critical Sensitive	Top Secret	Tier 5 (SSBI)[2]	Tier 5R (SSBI-PR or PPR)[2]	Every 5 years	3
Special Sensitive	Top Secret/SCI	Tier 5 (SSBI)[2]	Tier 5R (SSBI-PR or PPR)[2]	Every 5 years	4

[1]Except for a break in service of 2 years or more prior to reinstatement/reactivation. Under this break in service situation, the individual would be processed for a new Tier 1 investigation.

[2]Effective October 1, 2016, all tiered investigation naming conventions are in effect. Previous completed background investigations and background investigations opened before their respective naming convention transition dates will retain their original background investigation names (shown in parentheses).

ANACI: Access National Agency Check with Inquiries
BI: Background Investigation
MBI: Minimum Background Investigation
NACI: National Agency Check and Inquiries
NACLC: National Agency Check with Law and Credit
PPR: Phased Periodic Reinvestigation

PRI: Periodic Reinvestigation
PSI: Personal Subject Interview
SCI: Sensitive Compartmented Information
SSBI: Single Scope Background Investigation
SSBI-PR: Single Scope Background Investigation – Periodic Reinvestigation

D. **North American Electric Reliability Corporation (NERC) Requirements.** NERC Critical Infrastructure Protection (CIP) Standard CIP-004 requires individuals with unescorted access to Physical Security Perimeters (as defined and established under CIP-006) to undergo a Personal Risk Assessment every 7 years consisting of an identity verification and 7-year criminal check. Personal Risk Assessments are separate from the background reinvestigation requirements described above. Processes and procedures for conducting these Personal Risk Assessments are contained in NERC CIP policies and procedures.

E. **Responsibility for Background Investigations Costs.** Background investigation costs will be funded from appropriate administrative and program accounts where a position or program resides. An appropriate cost structure and organizational code/cost center will be provided at the time a background investigation is requested or initiated.

F. **Exceptions.**

(1) The following positions are excepted from these background investigation or upgraded investigation requirements (provided that any separate background investigation requirements of the HSPD-12 PIV process and any NERC-CIP requirements have been met):

(a) Positions which are intermittent, seasonal, per diem, or temporary (including details or temporary promotions), any of which is not expected to exceed an aggregate of 180 calendar days per 12-month period in either a single continuous appointment or a series of appointments. This does not preclude appropriate checks (e.g., verification of any issues in OPM's Central Verification System (CVS), fingerprint check, screening OF-306, etc.) conducted to ensure the suitability of an individual.

(b) Other positions that OPM, in its discretion, deems appropriate based on a written request to OPM by an agency head in whose agency the positions are located.

(c) Positions filled by foreign nationals employed outside the U.S.

(2) These exceptions do **not** apply to national security positions.

G. **Prior Investigations (Non-Reclamation Associated).** Whenever a favorable adjudication of a prior agency investigation cannot be verified and wherever possible,

to decrease costs, investigations completed by another Federal agency or Department bureau will be requested and reviewed to determine if the type of previous investigation meets the appropriate EO, Department, OPM, and Reclamation requirements for the new position or for serving in contracted roles. Reclamation will not consider prior investigations, when an individual has a break in service of 2 or more years since the previous investigation, the prior investigations do not meet the minimum investigation requirement according to the position sensitivity designation, a favorable adjudication cannot be verified, or the reinvestigation frequency of the prior investigation has been exceeded.

H. **Waiver of Pre-Appointment Investigation Requirement.**[1] The interest of the Federal service dictates that individuals must not be appointed or assigned to critical sensitive positions or LE positions until the appropriate investigation or waiver has been completed. Waiving a pre-appointment investigation carries the risk of an ineligible person being placed in a sensitive position exposing the Federal service to damage and embarrassment. EO 10450, as amended, requires that a waiver of the pre-appointment investigative requirement for employment in a "sensitive" position only be made “in case of emergency” provided that such action is necessary “in the national interest.” If a waiver is utilized, the manager will request a waiver of the pre-appointment investigation requirement for a critical sensitive position or LE position by completing all of the requirements as described below.

(1) Subject to the EO 10450 provisions for being an “emergency” and “in the national interest,” a Request for Waiver of Pre-appointment Investigative Requirement for a Critical Sensitive Position, Form DI 1912, (see Appendix B, page B1 for non-LE positions or B3 for non-critical sensitive/critical-sensitive LE positions) will be completed and approved before appointing or assigning an individual to a critical-sensitive position or LE position, unless the required background investigation has been completed. Waiver requests must be submitted to the SSLE Personnel Security Office, at a minimum, 2 weeks prior to the proposed effective date to ensure required checks and approval is obtained prior to entrance on duty. The specified required checks (see Appendix B, page B2 for non-LE positions or B4 for LE positions) must be completed by the requesting office.

(2) A waiver is required for each employee or individual assigned, transferred, demoted, reassigned, or promoted (whether permanently or as a temporary/term employee) to a critical sensitive position or LE position unless the appropriate level of background investigation has been fully completed in advance.

[1] A person currently holding a Top Secret clearance may be placed directly into a position requiring an SCI without a waiver while awaiting adjudication of the SCI.

(3) Waivers cannot be used for special sensitive positions.

(4) Waivers are optional for non-critical sensitive positions except for LE positions. Waivers are required for all LE positions unless a favorably adjudicated background investigation that meets the minimum requirement has been verified.

(5) Granting a waiver does **not** provide authorization for access to classified national security information or delegation of law enforcement authority.

(6) Before forwarding the applicable waiver request, the following mandatory specified checks/item/forms must be completed by the requesting office and results attached to Form DI 1912 (Appendix B, page B1 for non-LE positions or B3 for LE positions):

(a) Pre-appointment Background Check, Form DI 1990 (see Appendix B, page B2 for non-LE positions or B4 for LE positions);

(b) Questionnaire for National Security Positions, Form SF 86;

(c) current resume; and

(d) justification requesting a waiver of this pre-appointment investigative requirement which will:

(i) be written and state the necessity including the "emergency" necessitating the request and the rationale justifying it being in the "national interest";

(ii) include a statement that the employee will not have access to classified national security information; and

(iii) include a statement (when applicable) that the employee will not receive delegation of LE authority until notification is received from the CSO advising that the background investigation is complete and has been favorably adjudicated.

(7) The Request for Waiver of Pre-appointment Investigative Requirement for a Critical Sensitive Position (or non-critical sensitive/critical-sensitive for LE positions) will be forwarded to the SSLE Personnel Security Office according to the sequence designated on DI 1990 (Appendix B, page B2 for non-LE positions or B4 for LE positions). The submitting office will be notified of the action taken on the request by SSLE.

(8) Upon the approval of a waiver by the SSLE Director or designee (or the DOI Office of Law Enforcement and Security for LE officer positions), the individual

may enter on duty or be reassigned to the critical sensitive position or LE position; however, the required investigation must be initiated within 14 calendar days of the individual occupying the position.

7. **Investigative Forms.**

A. **General.** Various forms are used to request a background investigation. The form used is based on the type of position, i.e., the risk and sensitivity level, rather than the type of investigation to be performed. Investigative forms must be accessed and entered on-line via the Electronic Questionnaires for Investigations Processing System (e-QIP) at the following Web site: www.opm.gov/e-qip. Individuals must first be initiated into the system by a personnel security specialist or other authorized staff member.

B. **Descriptions.** The following Table 2 designates the various forms used in the background investigation process required by OPM to schedule an investigation. Table 3 identifies the documentation required to be provided to the SSLE Personnel Security Office for processing higher level investigation requests or paperwork required for verifying position sensitivity prior to processing a required reinvestigation.

Table 2:

Type of Position	SF 85	SF 85P	SF 86	OF 306*	Resume*	FTS**	FCRA
Non-Sensitive/ Low Risk	X			X	X *	X **	
Moderate or High Risk Public Trust		X		X	X *	X **	X
National Security			X	X	X *	X **	X

* Not required for reinvestigations for Federal employees.

** Fingerprint submissions will be submitted through authorized FTS. In the event the electronic fingerprints are unclassifiable after a second attempt, a hardcopy fingerprint card will be used (SF 87 for Federal employees; FD 258 for contractor staff). Fingerprint submissions are not required for national security reinvestigations.

FTS: Fingerprint Transmission System
SF 85: Questionnaire for Non-Sensitive Positions
SF 85P: Questionnaire for Public Trust Positions
SF 86: Questionnaire for National Security Positions
OF 306: Declaration for Federal Employment
SF 87: Fingerprint Card for Federal employment
FD 258: Non-Federal Employee Applicant Fingerprint Chart
FCRA: Fair Credit Reporting Act Authorization form
OF 8: Cover sheet to PD

Table 3:

Types of Background Investigation Requests	Background Investigation Request Form	Position Sensitivity Designation using OPM PDT Tool	OF 8 & PD	SF 50*****
Upgraded Background Investigations	X	X	X	X
Reinvestigations	X	X	X	X

***** Copy of Notification of Personnel Action (SF 50) reflecting the current sensitivity change may be provided at a later time if the action is pending.

8. **Adjudication.**

A. **General.**

(1) Adjudication is an assessment of an individual's past and present conduct to determine whether an individual is loyal, reliable, and trustworthy to promote the efficiency of the service (suitability), and when applicable, to determine the individual's eligibility for access to classified information (national security).

(2) The overall process objective is to adjudicate an individual's suitability for promoting the efficiency of the Federal service and, if applicable, is in the interest of national security while assuring "fair, impartial, and equitable" treatment to the applicant/employee. Delegated authority for Federal agencies from OPM for making most suitability determinations and taking most suitability actions for applicants and appointees is found in Title 5 CFR 731.103 and 731.105. Adverse action procedures taken on employees due to unfavorable suitability background investigations are found in 5 CFR 752. Adverse action procedures relating to national security positions are found in 5 CFR 732.301.

B. **Initial Suitability Screening.** During the hiring process or an applicable internal position action, the servicing HR office, or other office as designated by the Regional Director, screens job applications[2] to identify any potentially disqualifying suitability issues. The initial suitability screening and referral process occurs during the competitive examining process and prior to initiating an investigation. Cases involving potentially disqualifying issues are referred to qualified adjudicators for a determination of the person's employment suitability. Further information on the initial suitability adjudication and referral process is contained in 441 DM 5.2.

[2] Job applications refer to forms used prior to occupying a position, i.e., resume, e-QIP, OF-306, supplemental questionnaires, etc.

C. **Adjudication Process.** With the exception of the initial suitability screening described above and an advance favorably adjudicated fingerprint check provided by OPM, the formal adjudication process occurs after OPM completes the personnel investigation of an individual. Additional information on the adjudication process is contained in OPM's "Suitability Processing Handbook."

D. **Issue Seriousness Ranking System.** After OPM has gathered all of the information regarding a background investigation, it makes a preliminary adjudication and codes/ranks both the overall adjudicative character of the case and any specific potentially derogatory information (issues) developed during the course of its investigation based on levels of characterization seriousness. OPM informs Reclamation of its assessment upon completion of the investigation by referring to the following issue seriousness codes ranked as "A, B, C, or D" by OPM's Investigation Service:

(1) "A" issue(s) are Minor and the conduct or issue, standing alone, would not be disqualifying for any position under suitability.

(2) "B" issue(s) are Moderate and the conduct or issue, standing alone, would probably not be disqualifying for any position under suitability.

(3) "C" issue(s) are Substantial and the conduct or issue, standing alone, would probably be disqualifying for any position under suitability.

(4) "D" issue(s) are Major and the conduct or issue, standing alone, would be disqualifying for any position under suitability.

E. **Adjudication Standards.** Adjudication standards are contained in 441 DM 5 and the OPM Suitability Processing Handbook. These standards will also be applied when adjudicating contractor background investigations.

F. **Adjudicators.** Adjudication is performed by trained personnel security specialists, or in the case of low risk suitability adjudications, other specialists trained and experienced in adjudication (e.g., HR specialists or security officers). Specific adjudicative responsibilities are as follows:

Type of Position	Office Responsible for Adjudication
National Security	SSLE Security Office
Public Trust – high and moderate risk	SSLE Security Office
Non-Sensitive/Low Risk Federal employees and contractor staff	Servicing HR Office or other office as assigned by the regional director[1]

[1] SSLE is responsible for Denver and Washington Offices. Lower Colorado (LC) regional security office is responsible for LC region.

(1) At a minimum, the Graduate School USA Course "Suitability Adjudication" or an equivalent course is required for individuals conducting any level of suitability adjudication. Adjudicators must continue to receive periodic refresher training (e.g., seminars, conferences, special courses, etc.) every 3 years in order to keep well informed of the latest developments of the program.

(2) The individual conducting the review and adjudication must have been found suitable by obtaining, at a minimum, a favorably adjudicated national security moderate risk background investigation in accordance with OPM Position Designation Tool guidelines.

G. **Adjudicative Procedures.**

(1) The adjudicator will review OPM's investigation results and make an initial suitability determination recommendation.

(2) Upon request, the SSLE Personnel Security Office will conduct an adjudicative review of regional office adjudications that have a "C" or "D" seriousness ranking and any adjudication where the regional office adjudicator proposes a suitability denial.

(3) If an investigative report contains no information of a materially derogatory nature, the adjudicator signs and dates the OPM Certification of Investigation (COI). The COI is then sent to the servicing HR office (for Federal employees) to file in the individual's electronic-Official Personnel Folder (e-OPF). Employees and their supervisors are notified of the favorable adjudication. The adjudication office will maintain a copy of the COI in the security file. For contractor staff, the COI is retained by the adjudication office. The COR is notified of the favorable adjudication.

(4) Information about clearance and position risk/sensitivity level for national security and public trust positions including type and date of investigation, initiating reinvestigations, and other pertinent data will be maintained by SSLE.

(5) If an individual's investigative report contains materially derogatory information (issues), the adjudicator will do the following:

(a) Review the investigative report and synopsize the issues.

(b) As needed, generate a Letter of Interrogatory (LOI) (for suitability cases) or a Statement of Reasons (SOR) letter (for national security cases) to ascertain additional information for issue resolution. The LOI or SOR will be sent through Employee Relations (ER) staff in the servicing HR office for

submission to the employee in collaboration with the supervisor. For contractors, the LOI will be coordinated through the COR.

(c) The adjudication action taken will range from making a favorable determination (with or without contacting the individual for issue resolution) up to, and including, removal. No unfavorable action will be taken unless the conduct is not clearly consistent with the interests of national security or there is a nexus between the conduct and the required duties of the position which does not promote the efficiency of the Federal service, or with Reclamation's ability to perform its mission.

(6) The individual will have 30 calendar days (for suitability cases) or 45 calendar days (for national security cases) to respond to and resolve the identified issues. If progress is being made to address the issues, a single 30-day extension may be granted by the CSO. A second LOI or SOR is generated if new information is discovered requiring additional information from the individual. After the allotted period, a final adjudication will be made based on the information obtained.

(7) Upon receipt of an individual's responses to an LOI or SOR, the adjudicator will make a final adjudication based on the information obtained. This information will be maintained in the individual's security file. The adjudicator will consider all information furnished when making the final adjudication.

(8) If the investigative report containing materially derogatory information is on a current Reclamation employee who was previously found suitable for a public trust position or found eligible for a national security position, the following will occur. These actions listed below reflect that a general suitability and/or security determination is pending. If the individual has been contacted during this phase, the results of that contact are made a part of the individual's file.

(a) the SSLE Personnel Security Office will notify the ER office staff, and ER will contact the appropriate management/supervisory official.

(b) the management/supervisory official, in conjunction with servicing HR office/ER staff, will consider the appropriate action to take until a final adjudication determination is made.

(c) when appropriate, the employee's national security clearance will be temporarily suspended by the SSLE Personnel Security Office pending a final adjudication determination.

(9) For a current Reclamation employee in a public trust position converting to a national security position, the individual may remain in the public trust position

pending the outcome of the adjudicative process, or the individual can be placed in a non-critical sensitive national security position, but shall not have access to any classified information or material until a final determination is made.

(10) If an investigative report contains derogatory information concerning a Federal employee (transferee) in a non-national security position being transferred into a national security position, the individual shall not have access to any classified information or material until a final determination is made.

(11) For Federal employee suitability cases, if the final adjudication is unfavorable, the CSO will notify the supervisor/manager and servicing HR office/ER staff by sending an Adverse Suitability Determination Memorandum.

(12) For national security positions, if the final determination is unfavorable, the CSO will issue a Letter of Decision (LOD) to the individual with a copy to the servicing HR office/ER staff as notification of the unfavorable determination. The LOD outlines the individual's appeal rights to the DOI Personnel Security Appeals Board (PSAB). The servicing HR office will not take any adverse action unless the PSAB appeal process is completed and the decision upheld or an appeal is not filed within the allowable time period. The CSO will keep the servicing HR office/ER staff informed in a timely manner of the status. If the case is appealed, the servicing HR office/ER staff will be notified by the CSO of the final outcome of the appeal. If the appeal is upheld, an Adverse Security Determination Memorandum will be sent by the CSO to the supervisor/manager and servicing HR office/ER staff. For more specific information, refer to due process procedures as described in 441 DM 5.8.

(13) For contractor staff, if the final adjudication is unfavorable, the CSO will send an Adverse Suitability Determination Memorandum to the COR to ensure the removal of the individual from the contract and access to the Federal facility at which the contract activities are occurring.

(14) For national security positions, if the final determination is favorable, the CSO can reinstate the individual's temporarily suspended or revoked clearance, if applicable, and will notify the servicing HR office/ER staff about the reinstatement.

(15) If the adjudication process results in an individual being found unsuitable or ineligible for the position for which they are being considered, the supervisor/manager of that position must initiate one of two actions:

(a) Rescind any offer of employment for the position under consideration.

(b) Remove the individual from the position if they have already been placed in the position under consideration.

(16) Employees found unsuitable or ineligible for a position may not be placed into another vacant position which would be a promotion or grade increase from the position vacated through non-competitive means, nor requiring waiving minimal qualifications, impact priority placement, or lead to double encumbering. Such a determination may also not be used as the basis for changing the designation of the position to accommodate the unsuitable or ineligible individual. Note: Eligibility within this context refers to a national security clearance.

(17) The final adjudicative determination notice (INV Form 79A) will be provided to OPM or entered into CVS. A copy of the INV Form 79A and any adjudication notes or summary sheets will be filed in the individual's security folder.

9. **National Security Clearances.**

A. **General.** Reclamation's SSLE Personnel Security Office will ensure that an appropriate background investigation is conducted and favorably adjudicated, a security briefing is conducted, and an SF 312 is signed and witnessed prior to granting a security clearance.

B. **Need for Clearance.** A security clearance will only be granted to those individuals with a bona fide need to access classified information or who routinely work or need unescorted access to an area where classified material is used or stored. A clearance is generally not required for an individual that occasionally acts in, or is on a temporary detail to, a position designated as a national security position. However, a clearance is appropriate for individuals that would likely need access (in an acting capacity) to classified information or facilities in certain situations, such as continuity of operations. In these cases, the PD and position designation must identify that need and contain the proper risk and sensitivity level.

C. **Interim Security Clearances.** For positions that will have a need for temporary access to national security information, an interim security clearance can be granted so long as the EO requirements for an interim security clearance are met. Specific procedures for processing an interim security clearance in these cases can be ascertained on a case-by-case basis by contacting the SSLE Personnel Security Office. This is used infrequently and is only applied in emergency situations when required to support the mission of the organization.

D. **Prior Security Clearances.** Prior security clearances granted by other Federal agencies (including other Department components) automatically terminate and are administratively withdrawn when an employee transfers or is reassigned; however, if a favorably adjudicated investigation cannot be verified an investigation used by another agency as a basis to grant a clearance will be requested and reviewed, if available, to determine if the type of investigation previously conducted meets the appropriate

Department, EO, and OPM requirements for granting of a security clearance under reciprocity. When an employee transfers to Reclamation from another Federal agency, the losing agency's security file and/or investigative record can be transferred to Reclamation where it will be reviewed and utilized as a basis for determining that the transferring employee has already met the applicable investigative requirements. Transferring employees in need of Reclamation clearances will still need a new security briefing. Clearances are only granted by the gaining agency if the position duties and position sensitivity designation require it.

E. A contractor employee needing a national security clearance is processed under the National Industrial Security Program Operating Manual (NISPOM) as specified in 443 DM 1. DOI does not have the authority to grant clearances to contractors, therefore, all contractor clearance requests must be processed through the DOD NISPOM. For further information, refer to DOD NISPOM 5220.22-M dated February 28, 2006.

F. **Security Briefing.** When a clearance is granted, a security briefing will be conducted by an authorized security briefing officer. The following procedures will be used:

(1) A security briefing must be conducted before employment or work commences, or as soon as possible thereafter, but before the granting of a clearance. An individual will not have access to classified information until the security briefing is conducted. Responsibility for conducting security briefings may be delegated from the CSO to other SSLE Personnel Security Office staff, regional security officers, or other authorized security briefing officers.

(2) Security briefing materials, including the SF 312, will be provided to the employee by the security briefing officer. The security briefing materials will also outline the reporting requirements for individuals with security clearances. The Defense Human Resource Activity (DHRA) Web site (http://www.dhra.mil/perserec/osg/home.htm) is provided as part of the briefing materials which identifies what must be reported. Examples include, but are not limited to, arrests or incidents with law enforcement, foreign travel, foreign contacts requesting sensitive information, serious financial difficulties, and life changing events such as marriage, divorce, birth of a child, name change, change of address, etc.

(3) The employee will acknowledge understanding of his/her responsibilities listed in the SF 312 and will sign and date the form. When an individual signs the SF 312 form he/she is acknowledging that he/she are bound for life by a contract with the U.S. Government to not disclose any classified information. The form will be witnessed by the security briefing officer as a qualified witness who possesses an "equal to" or "higher level" security clearance as the individual signing the SF

312. The signed original SF 312 will be maintained by the SSLE Personnel Security Office.

G. **Granting.** Once the security briefing process is completed and upon the receipt of a properly executed and witnessed SF 312 by SSLE, the granting of a clearance is performed. The procedures are as follows:

(1) Verification of a properly executed SF 312, and

(2) Preparation of a grant letter by the SSLE Personnel Security Office staff and distributed as follows:

(a) original to the employee's e-OPF;

(b) copy to the employee;

(c) copy to the employee's supervisor; and

(d) copy to the employee's security file, which is retained by SSLE.

H. **Training.** In compliance with 32 CFR Part 2001 (*Classified National Security Information*), all employees and contractors who create, process, or handle classified information shall have refresher security education and training at least annually. This training will focus on the proper handling and protection of classified information.

I. **Travel Reporting Requirements.** All clearance holders are required to report all foreign travel. An e-mail notification to the SSLE Personnel Security Office identifying dates of travel, location of travel, and purpose of travel (i.e., official or non-official) must be provided. It is also required that prior to travel a clearance holder must review the U.S. Department of State Web site at http://travel.state.gov/content/travel/english.html to review any travel concerns or prohibitions that may exist for the specific foreign country they will be visiting.

J. **Security Debriefing.** Prior to a cleared individual separating from employment with Reclamation or upon a position sensitivity change no longer requiring the individual to have a national security clearance, a debriefing must occur. Procedures to accomplish the debriefing are as follows:

(1) The SSLE Personnel Security Office must be notified by the appropriate servicing HR office when an employee is separating (transferring or terminating) or being downgraded from a national security position. This also applies to reassignments within Reclamation (i.e., from region to region) as the position sensitivity often changes. For separations from Reclamation, notification must be by way of e-mail to the SSLE Personnel Security Office on the day the HR office is notified

of the scheduled separation. For position sensitivity changes, the HR office will provide to the SSLE Personnel Security Office a modified position sensitivity designation package as soon as possible. This is to ensure timely notification for the requirement of the employee to be debriefed prior to separation or downgrading from a national security position.

(2) The SSLE Personnel Security Office contacts the employee within 24 hours of notification to schedule an appointment for the debriefing or to make other arrangements if the employee is not available. If the employee to be debriefed is at a location other than in Denver, Colorado commuting area, arrangements are coordinated by the SSLE Personnel Security Office for a field security briefing officer to conduct the debriefing. All applicable documents are sent by the SSLE Personnel Security Office to the assigned security briefing officer for his/her use in this process; or, in the rare case when an employee has already separated, the debriefing will be accomplished via correspondence between the SSLE Personnel Security Office and the former employee.

(3) The debriefing is accomplished by the employee reading, signing, and dating the debriefing acknowledgement on the bottom of the original SF 312 with the security briefing officer witnessing this action. The debriefing officer will explain the continued importance, even in separation and cancellation of the clearance, of the contract between the individual and the U.S. Government to not disclose classified information. It will also be explained to the individual that clearances do not pass to another agency or private sector job (only verification of a prior background investigation) and will be administratively withdrawn. In the rare case where this is accomplished after the fact, the witnessing of the form is not conducted in person but acknowledged by the SSLE Personnel Security Office via a memorandum to the file once the SF 312 is returned.

(4) The SF 312 is then returned to the SSLE Personnel Security Office for filing of a copy of the SF 312 in the employee's security file and the PSSP database is updated at that time. The employee's national security access is deactivated at that time and administratively withdrawn in CVS.

(5) The retention for the original SF 312 is 50 years from the date of execution. The original SF 312, once an employee is debriefed, is retained in the SSLE Personnel Security Office.

K. **Verification of Security Clearances and Personnel Investigations.** Before an individual with a security clearance attends a meeting or activity at another agency that requires a national security clearance, the individual's clearance must be verified in CVS or certain information must be passed between agency personnel security officers. A verbal declaration of a clearance cannot be accepted.

(1) To ensure proper verification, Reclamation employees coordinating a classified briefing, conference, meeting, training, or other activity requiring a national security clearance (or unescorted access to a secure area where classified material may be present) must notify the SSLE Personnel Security Office at least 7 calendar days in advance of the date of the activity with the following information:

(a) proposed attendee name, social security number, citizenship, date and place of birth;

(b) organization(s) represented, purpose of the activity;

(c) date, location, and security level of the activity;

(d) official point of contact, contact telephone number, and fax number; and

(e) duration the clearance is expected to be needed (not to exceed 1 year).

(2) Reclamation employees who plan to attend a classified briefing, conference, meeting, training, or other activity outside Reclamation requiring verification of a national security clearance must notify the SSLE Personnel Security Office and provide the required information listed above. This information must be provided at least 7 calendar days in advance of the date of the activity.

(3) If the SSLE Personnel Security Office cannot verify the clearance information via CVS, personnel security officers for individuals from other agencies visiting Reclamation must provide, in addition to the above, the following via fax:

(a) type and date of latest investigation;

(b) adjudication date of latest investigation;

(c) level and date of clearance granted;

(d) name of granting agency; and

(e) name of investigating agency.

L. **Sanctions for Security Incidents/Infractions/Violations.** Protecting classified information shall be of paramount concern upon discovery of any security incident. When an incident is discovered, immediate action will be taken to secure and control any classified information involved. Sanctions can include suspension or revocation of security clearances, and potential disciplinary action, up to and including termination from Federal employment.

10. **Records Management.**

A. **General.** The SSLE Personnel Security Office, the servicing HR offices, and the regional security offices have the authorization to request and receive investigative files from OPM. These offices are responsible for protecting Privacy Act investigative records and case files and maintaining those records as required by Reclamation's information security and records retention policies.

B. **Dissemination of Investigative File.** Reclamation will not allow an individual access to his/her investigation files. The following requirements will be observed by Reclamation when furnishing information to each of the following individuals or entities:

(1) **The Individual of the Investigation.**

(a) Reclamation will provide the individual excerpts, summaries, or an analytical extract of information from the investigation report via written correspondence.

(b) Reclamation will not provide the individual a copy of the OPM or any other agency investigation report.

(c) A copy of the investigation report is available from the investigative agency under the provisions of the Privacy Act and/or Freedom of Information Act (FOIA) (see Paragraph 10.D.).

(2) **Another Agency's Authorized Official.**

(a) Reclamation will not release a copy of any investigative file, in whole or part, to an agency, an agency investigator, or other representative, unless approval has been obtained from the investigative agency (e.g., Defense Security Service, Federal Bureau of Investigation, OPM, etc.). Pursuant to Section (b)(7) of the Privacy Act of 1974, Reclamation will permit employees outside the agency, if authorized by law, to view security files if they have made a written request and have a need to know as determined by the SSLE Personnel Security Officer. The custodian of the information will maintain a record of each disclosure. The disclosure record will include the official's name, title, address of the individual or agency, the type of investigation conducted on the reviewer of the file, the disclosure/review date, and the reasons for disclosure and review.

(b) Reclamation will allow OPM investigators to review and summarize any investigative file maintained by Reclamation. Disclosures are not required for OPM investigators to review the file.

(3) **Agency Authorized Officials.**

(a) Pursuant to Section (b)(1) of the Privacy Act of 1974, Reclamation will permit officers and employees of the agency to view security files if they have a need to know, as determined by the SSLE Personnel Security Officer, in the performance of their duties. The custodian of the information will maintain a record of each disclosure.

(b) The custodian of the information will ensure no investigative material or reports are copied, placed in the subject's e-OPF, or taken out of the control of the custodian.

C. **Protection of Investigative Sources and Materials.** No classified or any other information which might compromise investigative sources, methods, or otherwise identify confidential sources, shall be disclosed to any individual, the individual's counsel or representative, or to any other person or entity not clearly authorized to have the information.

(1) Personal information collected from employees, applicants, appointees, non-Reclamation employees, etc., is protected by the Privacy Act of 1974.

(2) Other applicable regulations pertaining to the safeguarding of classified information will be strictly observed by all individuals.

D. **Release of Investigative Report.** Reports of Investigation are only releasable in accordance with the provisions of the Privacy Act and/or FOIA.

(1) A copy of an investigation is available by completing and faxing a FOIA/Privacy Act Record Request Form (INV-100) to OPM. The form and fax number are located at the following Web site http://www.opm.gov/forms/pdf_fill/inv100.pdf; or

(2) sending a written request to:

U.S. OPM / Federal Investigative Services / FOIA Office
P.O. Box 618
ATTN: FOIA/Privacy Act Officer
Boyers, PA 16018-0618

(3) The request must include the following information:

(a) the individual's complete name and any other names used;

(b) the individual's Social Security Number, date of birth, and place of birth;

(c) the individual's home mailing address of where to send the investigative file;

(d) the individual's day time telephone number; and

(e) the signature of the individual requesting the file.

E. **Physical Storage.** Reclamation security offices will store investigative and adjudication files in either a combination-locked cabinet, safe, or in other secured manner to prevent unauthorized access.

RECLAMATION
Managing Water in the West

RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: **02/05/2019** Release No. **511**

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

Reclamation Manual Release Number and Subject

SLE 01-01 Personnel Security and Suitability

Summary of Changes

In addition to the minor revisions listed below, the following revisions were needed to SLE 01-01, Appendix A on page A5 footnote 1 as follows:
--Delete "high risk Public Trust" and replace with "moderate risk National Security."
--Delete "Tier 4 (BI)" and replace with "T3 (MBI)."

Minor revisions:
1. Clarification on Top Secret clearance holders to be placed in a position requiring an SCI clearance. (6H & Appendix A)
2. Change to required reinvestigation forms. OPM does not require a resume or OF-306 reinvestigations and does not require fingerprint submissions for national security reinvestigations. (7B)
3. Make language clear on specific types of job applications, i.e., resume, e-QIP, OF-306, supplemental questionnaires (8B)
4. Investigation level of individual conducting review and adjudication changed to national security moderate risk in accordance with OPM Position Designation Tool change, which became effective September 2017. (8F)

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 01-01 pp 1-28	**SLE 01-01 pp 1-28**
Appendix A pp 1-5	**Appendix A pp 1-5**
Appendix A pp 1-4	**Appendix A pp 1-4**

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

Filed by: _____ Date: _____