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 applicable to Federal employees, contractor staff, and other individuals. 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 (Public Law 100-235); Chapter 3 and 73 of Title 5, U.S. Code; Title 5 Code of Federal Regulations (CFR) 731, 732, and 736; Executive Orders (EO), as amended, 10450, 10577, 12958, 12968, and 13467; OMB Circular A-130, Federal Information Processing Standards Publication 201; Government Organizations and Employees; Appendix III; Homeland Security Presidential Directive 12 (HSPD-12); and Departmental Manual (DM) Parts 441, 442, 443, 444, and 446.

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

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

1. **Introduction.**

   A. The Federal Government mandates by law, EO, Presidential Directives, regulations, and guidance that all applicants, appointees, Federal employees, contractors, and others are suitable for employment or assignment of work with the Federal government, and that the employment or assignment of work is consistent with national security. The Personnel Security and Suitability program 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 requirements of HSPD-12, and (4) general risk management of potential insider threats.

   B. This Directive and Standard (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 (Personnel Security and Suitability Requirements), 442 (National Security Information), 443 (Industrial Security Program), 444 (Physical Protection and Building Security), and 446 (Law Enforcement) (see http://elips.doi.gov/app_home/index.cfm?fuseaction=home); and 5 CFR Parts 731 (Suitability), 732 (National Security Positions), and 736 (Personnel Investigations).

2. **Applicability.** This D&S applies to all Reclamation applicants, appointees, and Federal employees, plus contractors, volunteers, and other individuals that require a background investigation pursuant to HSPD-12 Personal Identity Verification or other requirements.

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 results of a review of a completed background investigation.

   C. **Classified Information.** Classified Information, as defined by EO 12958, as amended, is information regardless of form that requires protection against unauthorized disclosure.

   D. **Clearance.** An authorization, granted in writing, to access Classified Information. Also referred to as Security Clearance or National Security Clearance. Note: A favorably adjudicated background investigation, by itself, does not convey a Security Clearance. See also adjudicative determination.

   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. **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 clearance process, eliminate the manual paper process, improve quality control, and provide end-to-end accountability.

   G. **Interim Security Clearance.** A certification based on partial investigative action that a U.S. citizen, who requires access to classified information, has been found eligible for and granted temporary (pending a final determination) access to classified information at a specified level under Federal standards.

   H. **National Security Clearance.** An administrative determination based upon the results of an investigation that an individual is trustworthy and may be granted access to classified information to the degree required in the performance of assigned duties in a position designated as a national security position. Also refer to Clearance.

I. **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 Reclamation the occupant of which 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.

(2) **Critical Sensitive Position.** Any position with a requirement for access to top secret information, including certain positions having investigative, law enforcement, or security functions.

(3) **Non-Critical Sensitive Position.** Any other 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.

J. **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, e.g., access is required for the performance of official duties.

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

L. **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.

M. **Reclamation Security Office.** The Denver office within Reclamation's Security, Safety, and Law Enforcement (SSLE) directorate where the management of Reclamation-wide security functions (including information, personnel, and physical security) resides. This does not include management of IT or communications security which is part of the Chief Information Officer directorate.

N. **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.

O. **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). With regard to information security and IT security, "sensitive" is a general term that refers to sensitive, but unclassified, data, information, or systems. Access to sensitive but unclassified information or systems does not require that the individual be placed in a national security position or be granted a national security clearance.

P. **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.

Q. **Suitability Screening.** The process of conducting an initial suitability review of an applicant or prospective candidate by the 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. This includes a review of the application material, OF-306 (Declaration for Federal Employment), any available security or suitability questionnaire (e.g., SF-85, SF-85P, or SF-86), and any other pre-employment hiring or security interview data.

R. **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.** Information that is more detailed is available in 441 DM 2.

A. **SSLE Security Office.** Reclamation's Chief Security Officer (CSO), as the senior Reclamation security official, has overall responsibility for Reclamation's Personnel Security and Suitability Program. 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 process. Specific personnel security responsibilities of the CSO include, but are not limited to, the following:

(1) background investigation processing and adjudication of all public trust, and national security positions for Federal employees and contractor staff;

(2) background investigation processing and adjudication of all low-risk positions for Denver and Washington Office Federal employees and contractor staff;

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

(4) providing guidance, consultation, collaboration, and training on matters pertaining to background investigation processing, differentiation of various levels of contract position risk designation, position risk/sensitivity designation in general, or suitability adjudication;

(5) processing of background investigation waiver requests by validating eligibility and processing for approval;

(6) ensuring compliance with all investigative requirements; and

(7) record-keeping maintenance

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.** Responsibilities include consultation with supervisors and managers on position risk/sensitivity designation (including contract positions), conducting or witnessing SF-312 security briefings and debriefings, assisting in the background investigation coordination/initiation process, and other personnel security/suitability activities that may be delegated by the CSO or assigned by their applicable regional director.

D. **Information Technology (IT) Policy and Security Office.** Responsibilities include:

(1) the establishment of risk baseline position designation recommendations for specific Reclamation IT positions (see Appendix A); and

(2) in consultation with supervisors and/or managers, providing guidance on adjustments to baseline position designations for IT positions where circumstances so deem them appropriate and prudent.

E. **Denver Human Resources (HR) Program Management Group.** This group is responsible for determining the program designation for all Reclamation programs as required by 441 DM 3. This group will also ensure consistency/oversight of servicing HR offices' implementation of position designations and related database and information reporting activities.

F. **Servicing Human Resources Offices.** The servicing HR offices, or other office as designated by the regional director, are responsible for ensuring that the risk/sensitivity level of all Reclamation positions are properly designated and appropriate background investigations are conducted for low risk positions, assisting in the initiation of the investigation process for all positions, and implementing final personnel actions related

to Position Risk/Sensitivity Designation and National Security Clearance and/or Background Investigation status for all Federal positions. Specific responsibilities are as follows:

(1) maintaining position designation information for Federal employee positions;

(2) performing initial suitability screening of all Federal employee positions (new hires, transferees, details, reassignments, temporary or permanent promotions, etc.) and all other individuals for whom HR initiates a background investigation whether the assignment is to an initial Reclamation assignment or position, or the assignment is to a different Reclamation assignment or position with a higher risk or sensitivity level;

(3) processing and adjudicating background investigations of Low-Risk Non-Sensitive positions for Federal employees and any other individuals (e.g., contract employees) where a director has assigned HR this responsibility;

(4) ensuring processing and compliance with all waiver requirements when applicable;

(5) reporting to the CSO any information (e.g., questionable conduct, financial misrepresentation, lack of trustworthiness, etc.) that may merit a follow-up adjudication to determine whether the individual's continued employment would be consistent with promoting the efficiency of government service; and

(6) record-keeping and related database and information reporting including immediate notification to the CSO 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 as non-national security.

G. **Managers and Supervisors.** Specific responsibilities are as follows:

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

(2) ensuring that the organization initiating a background investigation is provided all applicable data needed for processing the initiation of a background investigation;

(3) 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;

(4) ensuring timely compliance with all waiver requirements when applicable;

(5) reporting to the CSO any information that may indicate an individual's eligibility for access to classified information that appears to be inconsistent with the interests of national security; and

(6) reporting to a higher level management official, the HR Office and/or the Regional Security Office any information that may indicate an individual's eligibility for continued employment that appears to be inconsistent with the Public Trust in promoting the efficiency of government service.

H. **Acquisition Management Offices and/or Contracting Officers Technical Representatives (COTR) and/or Contracting Officer Representatives (COR).** Specific responsibilities are as follows:

(1) ensuring that all contracts under their authority include required Reclamation Acquisition Regulation security clauses;

(2) ensuring compliance with all investigation and reinvestigation requirements for contractor staff;

(3) assisting in the initiation of the personal identity verification process and background investigation process for contractor staff;

(4) as prescribed by the contract, taking action as a result of adverse suitability determinations of contractor staff; and

(5) coordinating with Contracting Officers on the mandatory utilization of the requirements of the National Industrial Security Program for any national security contracts as specified within 443 DM 1.

I. **Federal Employees and Contractor Staff.** All individuals are responsible for the following:

(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 the employee's supervisor or contactor's COTR, any job activities that they believe could result in a change in their position designation or their need for increased security access;

(3) reporting to the CSO, Regional Security Officer and/or HR Office, any information (i.e., personal conduct) that may appear to indicate an individual's (including their own) eligibility for any type of security access that is not consistent with prudent security practices;

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

(5) for individuals holding Top-Secret Clearances, reporting to the CSO any anticipated official and non-official travel to one or more of the following countries: Cuba, Iran, Libya, North Korea, Peoples Republic of China, Syria, and/or Vietnam; and

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

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 for assigning the impact and scope of operation for various Reclamation programs at one of four levels (Major, Substantial, Moderate, or Limited) as required by 441 DM 3. Program Designation is assigned by the HR Policy Management Team and is used in individual position designations.

C. **Position Designation.** The Department of the Interior's position risk/sensitivity designation system must be used to determine position risk/sensitivity designation (i.e., the national security sensitivity and/or suitability risk levels of a position.)

D. **Position Designation Levels.** Each Reclamation position will be designated and recorded on a position designation sheet, a position description cover sheet, and in the Federal Personnel Payroll System at one of six risk or sensitivity levels (non-sensitive/low risk, moderate risk, high risk, non-critical sensitive, critical sensitive, or special sensitive). Specific minimum position risk/sensitivity designation levels (along with corresponding background investigations, security clearances, and pre-appointment background investigation waiver requirements) for certain Reclamation positions are specified in Appendix A.

6. **Background Investigations.**

A. **General.** A background investigation is a written inquiry, telephone inquiry, and/or personal interview to determine an individual's suitability, eligibility, and qualifications for Federal 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) U.S. Office of Personnel Management (OPM) investigative references can be accessed at http://www.opm.gov/extra/investigate/.

(a) These investigations are conducted by OPM on behalf of Reclamation, although Reclamation can, when necessary (depending upon the circumstances), obtain investigations from a different Federal investigative agency.

(b) Investigations for Special Sensitive national security positions must be fully completed before placement in the position.

(c) Investigations for Critical Sensitive national security positions must be completed before placement in the position unless a waiver (see Paragraph 6.G.) of pre-appointment investigation is processed and approved.

(d) Investigations must be initiated within 14 calendar days of placement in the position. Investigation must be submitted within 30 calendar days from the date investigation was initiated.

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

(1) If an individual experiences a change in position risk/sensitivity level, (moves to a position with a higher level risk or sensitivity or the risk/sensitivity level of the position itself is changed) the individual may encumber or remain in the position for all levels of designation while the upgrade investigation is being conducted and adjudicated. (Note: Critical Sensitive positions require a waiver – see Paragraph 6.G.).

(2) By regulation (Title 5 CFR 731.106c, 732.201b and 732.202a2iv), any upgraded investigation required for a new risk/sensitivity level must be initiated within 14 calendar days of the effective date of the move or the new designation is finalized. Consequently, any upgrade investigation required for a new national security or public trust level must be transmitted to the Reclamation Security Office within 7 calendar days of the effective date.

C. **Types and Frequency of Investigations and Reinvestigations.** The following table gives the type of investigation and reinvestigation, and the frequency of reinvestigation that is 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 of the prior investigation.

Position Risk Designation	National Security Access	Background Investigation	Background Reinvestigation	Frequency of Reinvestigation
High Risk	None	BI	PRI	Every 5 years
Moderate Risk	None	MBI	NACLC	Every 10 years
Non-Sensitive/Low Risk	None	NACI	Not Applicable[1]	Not Applicable
Special Sensitive	Top Secret/SCI	SSBI	SSBI-PR or PPR	Every 5 years
Critical Sensitive	Top Secret	SSBI	SSBI-PR or PPR	Every 5 years
Critical Sensitive[2]	Secret[3]	SSBI	SSBI-PR or PPR	Every 5 years
Non-Critical Sensitive/ Moderate Risk	Secret	MBI	NACLC	Every 10 years
Non-Critical Sensitive/ Low Risk	Secret	ANACI	NACLC	Every 10 years

[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 NACI.
[2]Departmental Law Enforcement Officers are the only positions that are designated Critical Sensitive/Secret.

ANACI: Access National Agency Checks with Inquiries
BI: Background Investigation
MBI: Minimum Background Investigation
NACI: National Agency Check with Inquiries
NACLC: National Agency Check
PPR: Phased Periodic Review
PRI: Periodic Review with Inquiries
SSBI: Special Sensitive Background Investigation
SSBI-PR: Single Scope Background Investigation – Periodic Reinvestigation

D. **NERC Requirements.** North American Electric Reliability Corporation (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 seven years consisting of an identity verification and seven-year criminal check. Personal Risk Assessments are separate from the background reinvestigation requirements described above. Processes and procedures for conducting these Personal Risk Assessments will be contained in future 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 18-digit cost code 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 Personal Identity Verification process and any NERC Requirements have been met):

(a) Positions which are intermittent, seasonal, or temporary (including details or temporary promotions), any of which is not expected to exceed an aggregate of 180 calendar days in either a single continuous appointment or a series of appointments.

(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; and,

(c) Positions filled by aliens employed outside the United States.

(2) These exceptions do not apply to Critical Sensitive positions (see Paragraph 6.G.).

(3) These exceptions do apply to Non-Critical Sensitive positions as follows:

(a) For positions that will have a need for temporary access to national security information, an interim security clearance can be granted by meeting the EO requirements for an interim security clearance. Specific procedures for processing an interim security clearance in these cases can be ascertained by contacting SSLE on a case-by-case basis.

(b) For positions that will not have a need for temporary access to national security information, the individual can be placed in the position but shall not be authorized to access to national security information. This restriction shall be documented on the SF-50.

G. **Prior Investigations (Non-Reclamation Associated).** Wherever possible, and to decrease costs, investigations completed by another Federal agency or Department bureau will be requested and reviewed to determine if the type of previously conducted investigation meets the appropriate EO, Department, and OPM requirements for individuals occupying Reclamation positions or serving in contracted roles. Reclamation will not consider prior investigations, when more than 2 years have lapsed since the individual occupied the position that required the prior investigation, or the reinvestigation frequency of the prior investigation has been exceeded.

H. **Waiver of Pre-Appointment Investigation Requirement.** The interest of the Federal service dictates that individuals must not be appointed or assigned to Critical Sensitive positions until the appropriate investigation or waiver has been completed. Waiving a pre-appointment investigation carries the risk of an unsuitable person being placed in a sensitive position exposing the Federal service to damage and embarrassment. EO 10450, as amended, requires that waiver of the reappointment investigative requirement for employment in a "sensitive" position may 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 by completing all of the required checks for hiring a new employee or reassigning an existing employee to a position designated critical sensitive prior to the completion of the required investigation.

(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, Form 1) will be completed and approved before appointing or assigning an individual to a Critical-Sensitive position, unless the required background investigation (SSBI, SSBI-PR, or equivalent) has been completed. The specified required checks (see Appendix B, Form 2) must be completed by the requesting office; all remaining required checks will be completed by SSLE prior to approval.

(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 (subject to exceptions listed in Paragraph 6.E.) unless the appropriate level of background investigation has been fully completed in advance.

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

(4) 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 (see Appendix B, Form 1 or 1A):

(a) A Pre-appointment Background Check, Form DI 1990 (see Appendix B, Form 2);

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

(c) A resume, Optional Application for Federal Employment (OF 612), or any other written format of application meeting the specifications described in OF 510; and

(d) A justification requesting a waiver of this requirement which will:

(i) be written and state the necessity including the "emergency" necessitating the request and the rational 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 law enforcement authority until notification is received from the CSO advising that the background investigation is complete and has been favorably adjudicated.

(5) The "Request for Waiver of Pre-appointment Investigative Requirement for a Critical-Sensitive Position" will be forwarded to the CSO according to the sequence designated on DI-1990 (See Appendix B, Form 1). The submitting office will be notified of the action taken on the request by SSLE.

(6) Upon the approval of a waiver by the SSLE Director or designee (or Interior's Office of Law Enforcement, Security, and Emergency Management for Law Enforcement Officer positions), the individual may enter on duty or be reassigned to the critical sensitive position; however, the required investigation must be initiated within 14 calendar days of the individual occupying the position.

7. **Investigative Forms.**

A. **General.** This Paragraph describes the various forms that must be used when requesting a personnel 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 website: 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.** Reinvestigations or upgrades for current employees utilize the same forms except that the job application (OF-612, resume, or other application materials) and the OF-306 are not required. In addition, for national security reinvestigations on Federal employees, the fingerprint card (SF-87) is not required (unless the fingerprints submitted for the previous investigation were deemed unclassifiable). The following table designates the various forms used in the personnel investigation process.

Type of Position	SF 85	SF 85P	SF 86	OF 306	OF 612, * Résumé *	FTS, SF-87, FD-258	FCRA
Non-Sensitive	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 Contractor Staff.

** Fingerprint submissions will be submitted through authorized Fingerprint Transmission Systems (FTS) when available. In absence of FTS availability fingerprint card will be used. SF-87 for Federal Employees; FD-258 for Contractor Staff.

*** Not required for Contractor Staff, except for those designated at the Non-Sensitive/Low Risk level utilizing the SF-85. Only limited items (1, 2, 8 – 13, 16 & 17a) on the OF-306 are completed by contractor staff designated at the Non-Sensitive/Low Risk level utilizing the SF-85.

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
OF-612: Individuals' job application material or resume (OF-510 definition)
SF-87: Fingerprint Chart for Federal employment
FD-258: Non-Federal Employee Applicant Fingerprint Chart
FCRA: Fair Credit Reporting Act Authorization form

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 enough to promote the efficiency of the service (suitability), and when applicable, to determine the individual's eligibility for access to classified information.

(2) The overall process objective is to adjudicate an individual's fitness for promoting the efficiency of the service while assuring "fair, impartial, and equitable" treatment to the applicant/employee. Delegated authority for Federal agencies from OPM to take most suitability adjudicative determination is found in Title 5 CFR 731.103 and 731.105.

B. **Initial Suitability Screening.** During the HR hiring process or an applicable internal position action, the servicing HR office screens job applications to identify any potentially disqualifying suitability issues. The initial suitability screening and referral process occurs 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.

C. **Adjudication Process.** With the exception of the initial suitability screening described above and an advance National Agency Check (NAC) provided by OPM, the formal adjudication process occurs after OPM completes the personnel investigation of an individual.

(1) At a minimum, the USDA Graduate School Course "Suitability Adjudication" or an equivalent course is required for individuals conducting any level of suitability adjudication.

(2) The individual conducting the review and adjudication must possess a level of suitability that is, at a minimum, equal in scope and coverage with the investigative information being reviewed and adjudicated.

(3) Additional information on the adjudication process is contained in OPM's Suitability Adjudication 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. 441 DM 5 adjudicative 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

G. **Adjudicative Procedures.**

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

(2) All regional office adjudications that have a "C" or "D" seriousness ranking and any adjudication where the regional office adjudicator proposes a suitability denial may, at their discretion, be submitted to SSLE for adjudicative review and concurrence.

(3) The action taken may 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 there is a nexus between the particular conduct and the individual's performance, potential performance of duties, or with Reclamation's ability to perform its mission.

(4) If an investigative report contains no information of a materially derogatory nature, the adjudicator signs and dates the OPM Certification of Investigation (CIN). The CIN is then sent to the servicing HR office (for Federal employees) to file in the individual's Official Personnel File. The adjudication office will maintain a copy of the CIN. For contractor staff, a copy of the CIN will be sent to the HR office or COTR as designated by the Reclamation regional office.

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

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

(a) The adjudicator will review the investigative report and synopsize the issues.

(b) As needed, the adjudicator will conduct a personal interview with the individual to ascertain additional information for issue resolution. If this type of contact for information is needed and a face-to-face interview cannot be accomplished, a telephone interview will be conducted or an interrogatory letter will be sent to a verified address for the individual.

(7) The individual will have 30 calendar days 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. After the allotted period, a final adjudication will be made based on the information obtained.

(8) Upon completion of any adjudicative interview with the subject (or receipt of individual's responses to an adjudicative interrogatory letter), the adjudicator, after consulting with the CSO, 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.

(9) If the investigative report containing materially derogatory information is on a current Reclamation employee who is already certified for a Public Trust or national security position, the following will occur. (These actions 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 Security Office will notify the appropriate management official;

(b) the management official, in conjunction with HR, will consider whether or not to effect a personnel action to temporarily place the individual in a low-risk level position or modify the individual's current position so that only low-risk duties are performed; and

(c) when applicable, the employee's national security clearance will be temporarily suspended by SSLE pending a final determination.

(10) 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.

(11) 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 immediate access to classified information/material.

(12) For Federal employees, if the final (pre-due process) adjudication is unfavorable, the CSO will contact the applicable Reclamation Director to make them aware of the potential for initiating any personnel action that might be deemed necessary (i.e., temporary/permanently placement of the individual in a low-risk level position, disciplinary action, removal, etc.). Upon notifying the appropriate official, for national security related adjudications the adjudicator will initiate an internal Statement of Reasons (SOR) process as described in 441 DM 5.8 and inform the servicing HR Office, or refer the case to the servicing HR office for Unfavorable Suitability Determinations, if applicable.

(13) For contractor staff, if the final adjudication is unfavorable, the adjudicator will contact the applicable contracting authority to ensure removal of the individual from the contract and access to the Federal facility at which the contract activities are occurring, as prescribed by the contract.

(14) If the final determination is favorable, the CSO can reinstate the individual's temporarily suspended or revoked clearance and will notify the applicable manager about the reinstatement.

(15) The final determination notice (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.** A security clearance will only be granted to those individuals with a bonafide need to access classified information or who routinely work or need unescorted access to an area where classified material is used or stored. Reclamation's 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. A security briefing must be conducted before employment or work commences, or as soon as possible thereafter, but before the granting of a clearance. Responsibility for conducting security briefings may be delegated from the CSO to other SSLE staff, Regional Security Officers, or other authorized Security Briefing Officers. A contractor employee needing a national security clearance is processed under the National Industrial Security Program as specified in 443 DM 1.

B. **Prior Security Clearances.** Prior security clearances granted by other Federal agencies (including other Department components) automatically terminate when an employee transfers or is reassigned; however, an investigation used by another agency as a basis to grant a clearance will be requested and reviewed, as needed, 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.

C. **Security Briefing.** When a clearance is needed in the new position to which an individual is being assigned, a security briefing will be conducted by an authorized Security Briefing Officer. The following procedures will be used:

(1) Security briefing materials, including the Classified Information Non-Disclosure Agreement (SF-312), will be provided to the employee by the Security Briefing Officer.

(2) The employee will acknowledge understanding of his/her responsibilities listed in the SF-312 and will sign and date the form. The form will be witnessed by the Security Briefing Officer as a qualified witness which 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 Security Office.

(3) In addition to the hardcopy briefing materials, an optional security briefing video is also available. This optional video may be requested from SSLE.

D. **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.

(2) A grant letter is prepared by the personnel security staff and distributed as follows:

(a) original to the employee's Official Personnel Folder (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.

E. **Training.** In compliance with 32 CFR Part 2001 (Classified National Security Information Directive No. 1), all employees and contractors who create, process, or handle classified information shall have refresher security education and training at least annually. This training will be specifically focused on the proper handling and protection of classified information. Employees and contractors that have a national security clearance, but do not create, process, or handle classified information, are not required to have this annual refresher security education and training.

F. **Security Debriefing.** Prior to a cleared individual separating from employment with Reclamation or upon a manager's/supervisor's decision that an employee's position no longer warrants a need for a security clearance, a debriefing must occur. This is required by the applicable EO. Procedures to accomplish the debriefing are as follows:

(1) The CSO 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. Notification must be by way of e-mail to the SSLE personnel security staff on the day HR is notified of the separation. This is to ensure timely notification for the requirement of the employee to be debriefed prior to separation or downgrading.

(2) The SSLE personnel security staff contacts the employee immediately 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, CO, arrangements are coordinated by SSLE for a field Security Briefing Officer to conduct the debriefing. All applicable documents are sent by SSLE to the assigned Security Briefing Officer for their use in this process; or, in the rare case when an employee has already separated, the debriefing will be accomplished via correspondence between SSLE and the former employee.

(3) The debriefing is accomplished by the employee (or former employee) reading, signing, and dating the debriefing acknowledgement on the bottom of the original SF-312 with the Security Briefing Officer witnessing this action. In the rare case where this is accomplished after the fact, the witnessing of the form is not conducted in person but acknowledged by SSLE via a memorandum to the file once the SF-312 is returned.

(4) The SF-312 is then returned to SSLE 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.

(5) The retention for the original SF-312 is 50 years. The original SF-312, once an employee is debriefed, is filed in the employee's OPF on the right side for permanent record, prior to separation and/or transfer of the OPF to another facility. If the employee is transferred to another facility, the original SF-312 will be forwarded to the new agency or the National Personnel Records Center when necessary.

G. **Verification of Security Clearances and Personnel Investigations.**

(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 staff at least 7 calendar

days in advance of the date of the activity with the following information, unless Regional Security Officers are able to locally verify this information for their local participants:

(a) proposed attendee name, social security number, 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 passing of a national security clearance must notify the SSLE personnel security staff and provide the required information listed above. This information must also be provided at least 7 calendar days in advance of the date of the activity.

H. **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 actions as appropriate under Department and Reclamation policy.

10. **Records Management.**

A. **General.** A limited number of individuals within SSLE office, the servicing HR offices, the Regional Security Offices, and/or the servicing Acquisitions offices have the authorization to request and receive investigative files from OPM. These individuals are responsible for protecting these 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. An individual may request, under the provisions of the Privacy Act and/or Freedom of Information Act, copies of their files from the investigative agency. 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 may provide the individual excerpts, summaries, or an analytical extract of information from the investigation report.

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

(c) The individual can request a copy of the report from the investigative agency under the Freedom of Information or Privacy Acts.

(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., DSS, FBI, OPM, etc.).

(b) Reclamation will allow another agency's authorized investigator to review and summarize any investigative file maintained by Reclamation.

(c) Reclamation can furnish a summary of the file upon request.

(3) **Reclamation Officials.**

(a) A Reclamation official, who has a need to know, may be granted access by the SSLE personnel security staff (for low-risk cases, the applicable servicing HR Office or the Regional Security Office) to investigative information when performing his/her official duties.

(b) The custodian of the information will ensure the official has undergone a favorable background investigation commensurate in scope and coverage with the risk/sensitivity imposed by the nature of the investigative information reviewed.

(c) The custodian of the information will maintain a record of each disclosure. The disclosure record will include the official's name and title, the type of investigation conducted on the reviewer of the file, the disclosure/review date, and the reasons for disclosure and review.

(d) The custodian of the information will ensure no investigative material or reports are copied, placed in the subject's Official Personnel Folder (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 Freedom of Information Act.

(1) An individual may obtain a copy of their OPM investigation by sending a written request to: U.S. OPM / CFIS / FIPC
P.O. Box 618
ATTN: FOIA/PA Officer
Boyers, PA 16018-0618

(2) The request must include the following information:

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

(b) Social Security Number, date of birth, and place of birth;

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

(d) the individual's signature that is requesting the file.

E. **Physical Storage.** Reclamation will store investigative and adjudication files in either a combination-locked cabinet, safe, or in other secured manner to prevent unauthorized access. Access to personnel security files will be limited to authorized officials with a need-to-know.