

Reclamation Manual

Directives and Standards

- Subject:** Personnel Security and Suitability
- Purpose:** To describe the purpose, responsibilities, requirements, and procedures of Reclamation's Personnel Security and Suitability Program applicable to Federal Employees, Contractor Staff and other classification of individuals.
- Authority:** Executive Orders (EO), as amended, 10450, EO 10577, EO 12958, EO 12968; Public Law 100-235, Computer Security Act of 1987; Chapter 3 and 73 of Title 5, U.S. Code, Government Organizations and Employees; Title 5 Code of Federal Regulations (CFR) 731, 732, and 736; OMB Circular A-130, Appendix III; Homeland Security Presidential Directive (HSPD) 12; Federal Information Processing Standards Publication (FIPS PUB) 201; and Parts 441, 442 443, 444 and 446 of the Departmental Manual (DM).
- Contact:** Security, Safety, and Law Enforcement Office (SSLE), 84-45000.
-

1. Introduction.

- A. In 1953, EO 10450 established a government-wide security program. This Order was designed to ensure that the employment of present/future Federal employees is consistent with National Security. The Federal Government also mandates by law, EO, Presidential Directive, regulations, and guidance that all applicants, appointees, Federal employees, contractors, and others are suitable for employment or assignment of work with the Federal government. This program has three 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 security clearance, and (3) to implement certain Personal Identity Verification requirements of FIPS-201.
- B. This Directive and Standard (D&S) establishes policies and procedures which supplement and clarify the requirements and procedures for Reclamation in determining Personnel Security and Suitability matters contained in 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) of the DM (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, as well as contractors and other individuals that need a background investigation pursuant to Personal Identity Verification 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.

Reclamation Manual

Directives and Standards

- A. **Access.** One's ability to use, or opportunity to gain knowledge of, information, records, or data as required in the performance of official government business.
- B. **Classified Information.** Classified National Security Information that has been determined pursuant to EO 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked (CONFIDENTIAL, SECRET, OR TOP SECRET) to indicate its classified status when in documentary form.
- C. **Clearance.** An authorization, granted in writing, to access National Security information at a specified level (e.g., Confidential, Secret, Top Secret, etc.) Also referred to as Security Clearance or National Security Clearance. A favorably adjudicated background investigation, by itself, does not convey a Security Clearance.
- D. **Controlled Access Area (CAA).** CAAs are designated areas within a building or industrialized complex, such as a dam or powerplant, that contain sensitive equipment, controls, or operations. As an example, this includes (but may not be limited to) all primary and secondary operational control rooms, security control rooms, and Supervisory Control and Data Acquisition (SCADA) control rooms at National Critical Infrastructure (NCI) and Major Mission Critical (MMC) facilities.
- E. **Derogatory Information.** Information that indicates employment or continuing employment of an individual 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. **For Official Use Only (FOUO).** The official term used within Reclamation to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the national security of the United States and classified Confidential, Secret, or Top Secret under EO 12958, *Classified National Security Information*, as amended, or its predecessor or successor orders, is NOT to be considered FOUO. FOUO information is not to be considered classified.
- 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 at a specified level under Federal standards.
- H. **Low Risk ADP-C Position.** A non sensitive / low risk position of which the computer security duties do not rise to a moderate or high risk level. This level of position designation is treated as if it were a Public Trust position.

Reclamation Manual

Directives and Standards

- I. **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. See also “Clearance.”
- J. **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 sensitive positions of 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 and positions having investigative, law enforcement or security functions, or service on personnel security boards.
 - (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.
- K. **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.
- L. **Non-Sensitive/Low Risk Position.** Any position in Reclamation that does not fall within the definition of a National Security Position or Public Trust positions.
- M. **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.
- N. **Reclamation Security Office.** The Denver office within Reclamation’s SSLE directorate where the management of Reclamationwide security functions (including information, personnel, and physical security) resides. This does not include management of Information Technology (IT) or Communications security which is part of the Chief Information Officer directorate.

Reclamation Manual

Directives and Standards

- O. **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.
 - P. **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.
 - Q. **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.
 - R. **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 441DM5. 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.
 - S. **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 441DM2.
- A. **SSLE Security Office.** Reclamation’s Chief Security Officer, 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/debriefing process. Specific personnel security responsibilities of the Reclamation Security Officer include, but are not limited to, the following:
 - (1) Background investigation processing and adjudication of all ADP-C, Public Trust, and National Security positions for Federal Employees and Contractor Staff;

Reclamation Manual

Directives and Standards

- (2) Conducting security briefing/debriefings, and granting/verification of clearances;
 - (3) Providing advice, consultation, collaboration, and training (if requested) to Regional Security Officers, Contracting Officers Technical Representatives (COTR), Acquisitions staff, and HR staff on matters pertaining to the differentiation of various levels of contract risk designation, position risk/sensitivity designation in general, or suitability adjudication;
 - (4) Completion of background investigation waiver requests by processing for approval;
 - (5) Ensuring compliance with all reinvestigation requirements; and
 - (6) Record-keeping and related informational reporting supporting personnel security and suitability needs.
- B. Regional Security Officers.** Responsibilities include consultation with Supervisors and/or Managers on position risk/sensitivity designation, contract risk/sensitivity designation, assisting with and/or conducting/witnessing SF-312 security briefings and/or debriefings, and assisting in the background investigation coordination/initiation process and/or other personnel security/suitability activities that may be delegated by the Chief Security Officer.
- C. Information Technology Policy and Security Office.** Responsibilities include:
- (1) The establishment of baseline position designation recommendations for specific Reclamation IT positions (reference Appendix A); and
 - (2) In consultation with Supervisors and/or Managers, providing guidance on adjustments to baseline position designations for IT or IT related positions where circumstances so deem them appropriate and prudent.
- D. Denver Human Resources Program Management Group.** This team is responsible for determining the Program Designation for all Reclamation programs as required by DM441.3. This team will also ensure consistency/oversight of servicing HR offices implementation of position designations and related database and information reporting activities.
- E. Servicing Human Resources Offices.** The servicing HR offices 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, and implementing final personnel actions related to Position Risk/Sensitivity Designation, ADP-C status, and National Security Clearance and/or Background Investigation status for all Federal positions. Specific responsibilities are as follows:

Reclamation Manual

Directives and Standards

- (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.) whether the assignment is to an initial Reclamation position or the assignment is to a different Reclamation position with a higher risk or sensitivity level;
- (3) Background investigation processing and adjudication of Low-Risk Non-Sensitive positions for Federal Employees, except those designated as Low Risk ADP-C;
- (4) Ensuring compliance with all waiver requirements when applicable;
- (5) Reporting to the Reclamation Security Officer 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 Reclamation Security Officer 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.

F. 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 compliance with all investigation and reinvestigation requirements;
- (4) Ensuring compliance with all waiver requirements when applicable;
- (5) Reporting to the Reclamation Security Officer any information that may indicate an individual's eligibility access to classified information that appears to be inconsistent with the interests of National Security; and

Reclamation Manual

Directives and Standards

- (6) Reporting to a higher level management official and/or HR 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.

G. Acquisition Management Offices and/or Contracting Officers Technical Representatives and/or Contracting Officer Representatives. Specific responsibilities are as follows:

- (1) Ensuring that all contracts under their authority are properly designated for risk/sensitivity;
- (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, including providing the contractor with appropriate background investigation forms;
- (4) As prescribed by the contract, taking action as a result of adverse suitability determinations of contractor staff; and
- (5) Coordination with Contracting Officers on the mandatory utilization of the requirements of the National Industrial Security Program for any National Security contracts as specified within 443DM1.

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

- (1) Reporting to the employee's supervisor or contractor's COTR, any job activities that they believe could result in a change in their position designation or their need for increased security access;
- (2) Reporting to the Reclamation Security Officer, any information (i.e., personal conduct) that may appear to indicate an individual's (including their own) eligibility for any type of security access is not consistent with prudent security practices;
- (3) Assisting with and cooperating fully in any communications and/or forms completion related to the personnel security and/or suitability process;
- (4) Reporting to the Reclamation Security Officer by individuals holding positions covered by Top Secret clearances of any anticipated 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

Reclamation Manual

Directives and Standards

- (5) 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 the process of the HR Program Management Group for assigning the impact and scope of operation for various Reclamation programs at one of four levels (Major, Substantial, Moderate, or Limited). Further explanation is provided in 441DM3.
- C. **Position Designation.** The Department of the Interior's (DOI) 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.) For contract position designation, Reclamation Acquisition Regulation WBR 1452.237-80 requires that a risk/sensitivity level (low/med/high) be designated for the entire contract. Since individual position designations are not needed, the level of background investigation is determined based on the contract risk/sensitivity level.
- D. **Position Designation Levels.** 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. 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).

6. Personnel Investigations.

- A. **General.** A background investigation is a written inquiry, telephone inquiry, and/or personal contact 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) OPM's investigative references can be accessed at <http://www.opm.gov/extra/investigate/>.

Reclamation Manual

Directives and Standards

- (a) These investigations are conducted by U.S. Office of Personnel Management (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 for non-critical National Security and all Public Trust positions must be initiated within 14 days of placement in the position.

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.
- (2) By regulation (Title 5 CFR 731.106c, 732.201b and 732.202a2iv), any upgrade 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 Officer within seven calendar days of the effective date.

- C. Types and Frequency of Investigations and Reinvestigations.** 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. 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.

Reclamation Manual

Directives and Standards

Position Risk Designation	National Security Access	Personnel Investigation	Personnel Reinvestigation	Frequency of Reinvestigation
High	None	BI	PRIR ¹	Every 5 years
Moderate (high points) ¹	None	LBI ¹	PRI ¹	Every 10 years ¹
Moderate (low points)	None	MBI	NACI+C ¹	Every 10 years ¹
Low Risk ADP-C ²	None	NACI+C ^{1,2}	NACI+C ¹	Every 15 years ¹
Low Risk Non-Sensitive	None	NACI	Not Applicable ³	Not Applicable
Special Sensitive	Top Secret/SCI	SSBI	SSBI-PR	Every 5 years
Critical Sensitive	Top Secret	SSBI	SSBI-PR	Every 5 years
Critical Sensitive ⁴	Secret	BI	PRIR ¹	Every 5 years
Non-Critical Sensitive	Secret	ANACI ⁵	NACLC ⁵	Every 10 years

¹This represents a higher level investigation/reinvestigation and/or period than required under 44IDM3. The differentiation between “high-point” and “low point” is properly discerned by a full understanding of the OPM guidance for the point application process of position risk designation.

²Minimum level for any position with FISMA (IT Security) duties at or above the level of a super user.

³Except 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.

⁴DOI Law Enforcement Officers and all other positions with a need for access to National Security information up to the Secret level that have a High Risk Public Trust designation component.

⁵Table entries are for Non-Critical Sensitive/Low Risk positions only. Exceptions include: initial investigation for a Moderate risk (high points) Public Trust positions with a need for access to National Security information up to the Secret level is a LBI (reinvestigation is a PRI); initial investigation for a Moderate risk (low points) Public Trust positions with a need for access to National Security information up to the Secret level is a MBI (reinvestigation is a NACLC).

D. Responsibility for Background Investigations Costs. Background investigations costs will be funded from appropriate administrative and program accounts where a position or program resides.

E. Exceptions.

- (1) The following positions are excepted from these requirements, provided that all provisions of the Personal Identity Verification process 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 days in either a single continuous action or appointment (or series of actions or 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) Position filled by aliens employed outside the United States.
- (2) Individuals under any of these exceptions who are determined to need temporary access to National Security information may be permitted to receive an interim security clearance for access to classified information by meeting the EO

Reclamation Manual

Directives and Standards

allowance 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. Absent having been granted an interim security clearance, any individuals occupying positions under any of the exceptions listed above are not authorized for access to National Security information or unescorted access to CAAs.

- F. **Prior Investigations (Non-Reclamation Associated).** Wherever possible, and to decrease costs, investigations completed by another Federal agency will be requested and reviewed to determine if the type of previously conducted investigation meets the appropriate EO, DOI, and OPM requirements for individuals occupying Reclamation positions or serving in contracted roles.
- G. **Waiver of Pre-Appointment Investigation Requirement.** The interest of the Federal service dictates that individuals should not be appointed or assigned to Critical Sensitive positions until the appropriate investigation 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.” A manager may 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 checks [See Appendix B Form 2] are to be completed by the requesting office and are required; all remaining required checks will be completed by SSLE prior to approval. Granting a waiver does not provide authorization for access to classified national security information and/or delegation of law enforcement authority. Such a waiver is required for each new employee, transferee, individual demoted/reassigned/promoted (all whether permanently or as a temporary/term employee) assigned 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.
 - (2) Before forwarding the waiver request, the following mandatory specified checks/item/forms are to be completed by the requesting office and results attached to Form DI 1912 (see Appendix B Form 1):

Reclamation Manual

Directives and Standards

- (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 justifications 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 bureau/office security officer advising that the background investigation is complete and has been favorably adjudicated.
- (3) The “Request for Waiver of Pre-appointment Investigative Requirement for a Critical-Sensitive Position” will be forwarded to the Reclamation Security Officer 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.
- (4) Upon the approval of a waiver by the SSLE Director or designee, the individual may enter on duty or be reassigned to the critical sensitive position; however, the required investigation must be initiated within 14 days of the individual occupying the position.

7. Investigative Forms.

A. **General.** This section 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.

- (1) Investigative forms can be accessed at one of the following sites:
<http://www.opm.gov/forms/INDEX.asp> or
<http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?pageTypeId=8199&channelPage=ep/channel/gsaOverview.jsp&channelId=-13253>.

Reclamation Manual

Directives and Standards

- 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 *	SF-87, FD-258	FCRA
Non-Sensitive	X			X	X *	X **	
Low (ADP-C), Moderate or High Risk Public Trust		X		X ***	X *	X **	X
National Security			X	X ***	X *	X **	X

* Not required for Contractor Staff.

** 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.

SF 85: Questionnaire for Non-Sensitive Positions

SF 85P: Questionnaire for Public Trust Positions

SF 86: Questionnaire for National Security Positions

SF 86C: Standard Form 86 Certification (very limited use)

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 Title 5 CFR 731.103 and 731.105.

Reclamation Manual

Directives and Standards

- B. Initial Suitability Screening.** During the HR examining process, the initial consideration by a servicing HR office of an application, 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. In cases of material falsification, OPM retains the adjudication responsibility. Further information on the initial suitability adjudication and referral process is contained in 441DM5.2.
- C. Adjudication Process.** With the exception of the initial suitability screening described above, the adjudication process occurs after OPM completes the personnel investigation of an individual.
- (1) Cleared, experienced, and trained Reclamation Personnel Security Specialists assess an individual's eligibility for access to National Security information and/or employment suitability, or in the case of low risk suitability adjudications, trained and experienced HR Specialists assess an individual's employment suitability.
 - (2) Additional information on the adjudication process is contained in OPM's Suitability Adjudication Handbook that is referenced in the USDA Graduate School Course "Suitability Adjudication." At a minimum, this course or an equivalent course is highly recommended for individuals conducting any level of suitability adjudication.
- 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.

Reclamation Manual

Directives and Standards

(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 441DM5. 441DM5 adjudicative standards are also to be applied when adjudicating contractor background investigations. These guidelines have been recently revised by a Whitehouse issuance in December 2005.

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

Type of Position	Office Responsible for Adjudication
National Security	SSLE Security Office
Public Trust – high and moderate risk Low Risk ADP-C	SSLE Security Office
Non-sensitive / Low Risk (non ADP-C) Federal employees	Servicing HR Office
Non-sensitive / Low Risk (non ADP-C) Contractor staff	Servicing HR Office or as assigned by each Region

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 will then be sent to the servicing HR office (for Federal employees) to file in the individual’s Official Personnel File. The adjudication office may maintain a copy of the CIN. For contractor staff, the CIN will be sent to the servicing COTR office to file in the COTR’s official contract file with a copy sent to the servicing HR office or other designee.

Reclamation Manual

Directives and Standards

- (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 synopsise 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 work address for the individual.
- (7) Upon completion of any adjudicative interview with the subject (or receipt of subject's responses to an adjudicative interrogatory letter), the adjudicator, after consulting with the Reclamation Security Officer, 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. This is not required for Non-Sensitive/Low Risk cases.
- (8) 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 and the appropriate Director 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.
- (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 may not have access to any classified information or material until a final determination is made.

Reclamation Manual

Directives and Standards

- (10) If an investigative report contains derogatory information concerning a current non-Reclamation Federal employee (transferee) in a non-National Security position being transferred into a National Security position, the individual may not have immediate access to classified information/material. The Reclamation Security Officer will advise/suggest the regional HR Officer suspend further selection processing until a final determination is made.
- (11) At their discretion and upon receipt of the determination by SSLE that would result in a Public Trust or National Security denial, the servicing HR office or the applicable manager can request a second review by a different adjudicator of any adjudication that results in a proposed Public Trust or National Security denial.
- (12) For Federal employees, if the final (pre-due process) adjudication is unfavorable, the Reclamation Security Officer 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 441DM5.8 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 Reclamation Personnel Security Officer or the adjudicator (for Non-Sensitive/Low Risk cases) 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 Reclamation Security Officer can reinstate the individual's temporarily suspended or revoked clearance or certification and will notify the applicable Reclamation Director 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 should be conducted before employment or work commences, or as soon as possible thereafter,

Reclamation Manual

Directives and Standards

but before the granting of a clearance. Responsibility for conducting security briefings may be delegated from the Reclamation Security Officer to other SSLE staff, Regional Security Officers, or other authorized Security Briefing Officers. A Contractor needing National Security clearances is processed under the National Industrial Security Program as specified in 443DM1.

- B. Prior Security Clearances.** Prior security clearances granted by other Federal agencies (including other DOI 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 DOI, EO, and OPM requirements. More explicitly, when an employee transfers to Reclamation from another Federal agency, as needed and upon SSLE's written request, 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 and upon any one of the scenarios listed below, a security briefing will be conducted by an authorized Security Briefing Officer.

(1) Security Briefing Scenarios:

- (a) Favorable adjudication of a Reclamation - requested background investigation at an applicable level and scope;
- (b) Verification of an existing unexpired background investigation at an applicable level and scope; or
- (c) Receipt and favorable review (and adjudication if needed) by SSLE of an applicable level and scope of an existing unexpired background investigation that is not verifiable without a hands-on review.

(2) Security Briefing Procedures:

- (a) Security briefing materials including the Classified Information Non-Disclosure Agreement (SF-312 - See http://www.archives.gov/isoo/security_forms/standard_form_312.pdf) are provided to the employee by SSLE; and
- (b) The employee (after acknowledging their understanding of their responsibilities listed in the SF-312) will sign and date it as witnessed by a Security Briefing Officer as a ; (a qualified witness which possesses an "equal to" or "higher level" security clearance as the individual signing the

Reclamation Manual

Directives and Standards

SF-312.) 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 File (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. **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 Reclamation Security Officer 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 should 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; and
 - (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

Reclamation Manual

Directives and Standards

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 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. The retention for the 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. This should be done prior to separation and/or transfer of OPF to another facility, but will be forwarded to the new agency or the National Personnel Records Center when necessary.

F. Verification of Security Clearances and Personnel Investigations. 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 of the activity with the following information:

- (1) Proposed attendee name, social security number, date and place of birth;
- (2) Organization(s) represented, purpose of the activity;
- (3) Date, location and security level of the activity;
- (4) Official point of contact and contact telephone number and fax number; and
- (5) Duration the clearance is expected to be needed (not to exceed 1 year).
 - (a) Provided this data at least seven days in advance of the date of the activity.
 - (b) Meetings where the Regional Security Officers are able to locally verify this information for their local participants are exempt from this requirement.
 - (c) Reclamation employees who plan to attend a classified briefing, conference, meeting, training, or other activity outside Reclamation requiring a National Security clearance must notify the SSLE personnel security staff of the following information: date of the activity, location of the activity, duration the clearance is expected to be needed at this location for this activity (not to exceed 1 year), official point of contact and telephone number, and the contact's facsimile telephone number. This information should also be provided at least seven days in advance of the date of the activity.

G. Sanctions: Security Incidents/Infractions/Violations and Effects on Clearances. 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

Reclamation Manual

Directives and Standards

secure and control any classified information involved. Sanctions may include suspension or revocation of security clearances, and potential disciplinary actions as appropriate under DOI and Reclamation policy.

10. Records Management.

- A. **General.** A limited number of individuals within SSLE, the servicing HR 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 records retention policies.
- B. **Dissemination of Investigative File.** Reclamation will not allow an individual access to their 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 Subject of the Investigation.**
 - (a) The subject may be provided excerpts, summaries, or an analytical extract of information from the investigation report.
 - (b) The subject will not be provided, by Reclamation, a copy of the OPM or any other agency investigation report.
 - (c) The subject may request the report in writing from the investigative agency if he/ she wants a copy of the case 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 may furnish a summary of the file.
 - (3) **Reclamation Officials.**

Reclamation Manual

Directives and Standards

- (a) A Reclamation official, who has a need to know, may be granted access by the SSLE personnel security (for Low Risk cases, the applicable servicing HR office) staff to investigative information when performing his/her official duties.
 - (b) The SSLE 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 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 which includes all of the following:
 - (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.
 - (d) The individual's signature that is requesting the file.

Reclamation Manual

Directives and Standards

- (2) The request is sent to: U.S. OPM / CFIS / FIPC
P.O. Box 618
ATTN: FOIA/PA Officer
Boyers, PA 16018-0618

- E. **Physical Storage.** Reclamation will store investigations in either a combination-locked cabinet, safe or in other secured areas deemed to be equivalent by SSLE. Access to investigations will be limited to authorized Reclamation Personnel Security staff.