MANUAL TRANSMITTAL

10.23.1

Department of the Treasury
Internal Revenue Service

FEBRUARY 3, 2020

EFFECTIVE DATE

(02-03-2020)

PURPOSE

(1) This transmits revised IRM 10.23.1, National Security Positions and Access to Classified Information.

MATERIAL CHANGES

(1) IRM section title changed from Personnel Security to National Security Positions and Access to Classified Information. Subsections were relocated, reformatted, or organized to improve readability in compliance with IRM 1.11.2.3. See Exhibit 10.23.1-1 for a crosswalk of subsection moved between IRM 10.23.1 and IRM 10.23.3. See Exhibit 10.23.1-2 for a crosswalk of previous and current title/subsections that were changed.

(2) IRM 10.23.1.1 - Internal controls added in compliance with IRM 1.11.2. Included information related to the program owner, authority, roles/responsibilities, acronyms, and security terms/definitions.

(3) IRM 10.23.1.2 - New section added to describe a national security position and provide examples of such positions.

(4) IRM 10.23.1.3 - Guidance about national security position sensitivity and investigative levels relocated from IRM 10.23.3 as the subject matter relates to the guidance in this IRM.

(5) IRM 10.23.1.4 - Guidance about investigations for national security positions relocated from IRM 10.23.3 as the topic relates to subject matter in this IRM.

(6) IRM 10.23.1.5 - Guidance updated to reflect new requirements for reciprocally accepting investigations and adjudications completed /conducted by an authorized investigative/adjudicative agency.

(7) IRM 10.23.1.6 - Guidance updated to describe reinvestigation time periods for employees with access to classified information or who occupy a sensitive position.

(8) IRM 10.23.1.7 - New section added to provide guidance about continuous evaluation which requires periodic automated record searches be conducted to determine continued national security eligibility.

(9) IRM 10.23.1.8 - Guidance revised to reflect new reporting requirements, personal and foreign activities, for employees occupying a national security position.

(10) IRM 10.23.1.9 - New section added to describe the requirements for establishing/ maintaining personnel security records for employees in a national security position. Created subsections and moved existing subject matter to this section.

(11) IRM 10.23.1.11 - Information updated to clarify guidance about determining eligibility to access classified information or hold a sensitive position. Updated information about possession of foreign passport - Employees no longer have to surrender/destroy foreign passports while holding a national security position.

(12) IRM 10.23.1.12 - Guidance updated to include the Department of Treasury's authority to grant access for specific IRS positions and access to Sensitive Compartmented Information (SCI) for IRS employees.

(13) IRM 10.23.1.13 - Information updated to clarify guidance about the limitations of requesting and approving access to classified information.

(14) IRM 10.23.1.14 - Guidance updated to remove requirements for interim Top Secret as agency is no longer authorized to grant such access.

(15) IRM 10.23.1.15 - New section added to describe mandatory security awareness training requirements for the initial and continued access to classified information.

(16) IRM 10.23.1.16 - New section added to explain that employees with access to classified information at the Top Secret or Secret level will be subjected to random drug testing.

(17) IRM 10.23.1.19 - Information updated to clarify the requirements for administratively terminating access when an employee no longer requires access to classified information to perform official duties and receiving a security debriefing.

(18) IRM 10.23.1.20 - Guidance updated to include situations when an employee's access to classified information or eligibility to hold a sensitive position must or can be suspended.

(19) IRM 10.23.1.21 - Guidance updated about the delivery, receipt, and filing of the Notice of Review for denial or revocation of access to classified information or eligibility to hold a sensitive position.

(20) Throughout the IRM - Updated links, improved grammar and made other editorial changes.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 10.23.1, *Personnel Security*, dated August 5, 2016.

AUDIENCE

All employees who have access to classified information or hold a sensitive position and IRS operating and functional divisions that employ such employees.

Robin Bailey, Jr.
IRS Human Capital Officer

10.23.1
National Security Positions and Access to Classified Information

Table of Contents

10.23.1.1 Program Scope and Objectives
10.23.1.1.1 Authority
10.23.1.1.2 Roles and Responsibilities
10.23.1.1.3 Commonly Used Acronyms
10.23.1.1.4 Security Terms and Definitions
10.23.1.2 National Security Positions
10.23.1.2.1 Movement from a Public Trust Position to a National Security Position
10.23.1.3 Position Sensitivity and Investigative Levels
10.23.1.4 Investigations for National Security Positions
10.23.1.5 Reciprocity of Background Investigations and National Security Adjudications
10.23.1.6 Reinvestigations for National Security Positions
10.23.1.7 Continuous Evaluation
10.23.1.8 Reporting Personal and Foreign Activities
10.23.1.9 Personnel Security Records
10.23.1.9.1 Certificate of Clearance and/or Security Determination
10.23.1.9.2 Classified Information Non-disclosure Agreement (SF 312)
10.23.1.9.3 Written Consent Form for Access to Financial Records
10.23.1.9.4 Protection of Personnel Security Records
10.23.1.10 Prerequisites for Eligibility to Access Classified Information
10.23.1.11 Determining Eligibility for Access to Classified Information or to Hold a Sensitive Position
10.23.1.11.1 Possession of Foreign Passport
10.23.1.12 Authority to Grant Access to Classified Information or Eligibility to Hold a Sensitive Position
10.23.1.13 Limitations of Access Eligibility
10.23.1.14 Interim Eligibility for Access to Classified Information
10.23.1.14.1 Interim Access to Confidential or Secret Information
10.23.1.15 Mandatory Security Awareness Training for Access to Classified Information
10.23.1.16 Random Testing for Employees with Access to Classified Information
10.23.1.17 Protection of Whistleblowers with Access to Classified Information
10.23.1.18 Security Clearance Verification
10.23.1.19 Termination of Access to Classified Information
10.23.1.20 Suspension of Access to Classified Information or Eligibility to Hold a Sensitive Position
10.23.1.20.1 Notice of Suspension to the Employee
10.23.1.20.2 Notice of Suspension to the Supervisor
10.23.1.21 Denial or Revocation of Access to Classified Information or Eligibility to Hold a Sensitive Position
10.23.1.21.1 Notice of Determination

10.23.1.21.2 Review of Determination
10.23.1.21.3 Appeal of Determination

Exhibits
10.23.1-1 IRM 10.23.1 and IRM 10.23.3 Subsection Relocation Crosswalk
10.23.1-2 IRM 10.23.1 Previous and Current Title and Subsection Crosswalk

10.23.1.1
(02-03-2020)
Program Scope and Objectives

(1) **Purpose**. This section establishes general policy and procedures for national security position requirements, the retention and protection of personnel security records, and national security eligibility for access to classified information or to hold a sensitive position. The Associate Director, Personnel Security (PS) will maintain personnel security operations in accordance with the procedures outlined herein.

(2) **Audience**. This IRM is for all IRS Business Units.

(3) **Policy Owner**. Personnel Security (PS), Employment, Talent, and Security (ETS).

(4) **Program Owner**. PS is responsible for overseeing the Personnel Security program and providing policy and procedures related to personnel security matters.

(5) **Contact Information**. Website at:
Personnel Security, Who to Contact

10.23.1.1.1
(02-03-2020)
Authority

(1) The following authorities and sources are the basis for the established policy and procedures related to national security positions and access to classified information.

a. Title 5, Code of Federal Regulation (CFR), Part 1400, *Designation of National Security Positions.*
b. Title 5, CFR, Part 731, *Suitability*.
c. Executive Order (EO) 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*
d. EO 13764, *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-wide Governance Structure and Processes for Security Clearance, Suitability and Fitness for Employment, and Credentialing, and Related Matters*.
e. EO 12968, *Access to Classified Information*.
f. Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*.
g. SEAD 4, *National Security Adjudicative Guidelines*.
h. SEAD 6, *Continuous Evaluation*.
i. SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*
j. *Treasury Security Manual, Treasury Directive Publication 15-71*.
k. IRM 10.9.1, *National Security Information*.
l. Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information*.

10.23.1.1.2
(02-03-2020)
Roles and Responsibilities

(1) The responsibility for adjudication of background investigations for IRS applicants/employees who occupy a national security position falls under the jurisdiction of the Associate Director, PS.

(2) The IRS Human Capital Officer is the deciding authority who is responsible for reviewing any reply, from the applicant/employee, when eligibility to occupy a national security position is denied or revoked by the Associate Director, PS.

(3) The Treasury Security Appeals, Department of the Treasury (Treasury), is responsible for resolving the eligibility decision if the deciding authority affirms the decision to deny or revoke eligibility to occupy a national security position.

10.23.1.1.3
(02-03-2020)
Commonly Used Acronyms

(1) The table lists commonly used acronyms used throughout this IRM.

Acronym	Definition
CE	Continuous Evaluation
CFR	Code of Federal Regulations
EO	Executive Order
FOIA/PA	Freedom of Information Act/ Privacy Act
NDA	Non-Disclosure Agreement
OPF	Official Personnel File
OSP	Office of Security Programs (Treasury)
PS	Personnel Security
SCI	Sensitive Compartmented Information
SEAD	Security Executive Agent Directive
SF	Standard Form
SSO	Special Security Office (Treasury)
TD P	Treasury Directive Publication

10.23.1.1.4
(02-03-2020)
Security Terms and Definitions

(1) A list of security terms and definitions can be found at IRM 10.23.2.23, Security Terms and Definitions.

10.23.1.2
(02-03-2020)
National Security Positions

(1) A national security position is any position in which an incumbent could cause, by virtue of the nature of the position, a material adverse effect on the national security regardless of whether the individual has access to classified information. Such positions include those requiring eligibility for access to classified information and other positions include, but are not limited to, those with duties related to:

- Protecting the nation, its citizens, and residents from acts of terrorism, espionage, or foreign aggression
- Law Enforcement, public safety, criminal justice
- Protection or controlling access to facilities or information systems
- Investigative or adjudicative duties for national security, suitability, or fitness

10.23.1.2.1
(02-03-2020)
Movement from a Public Trust Position to a National Security Position

(1) If an employee, in a public trust position, requires access to classified or sensitive information to perform assigned duties, the following must be completed before the employee moves to a national security position.

a. The public trust position designation must be re-designated to the appropriate national security sensitivity level (Non-Critical Sensitive, Critical Sensitive, Special Sensitive) and/or the security clearance (Top Secret, Secret, Confidential).
b. Managers must immediately initiate a personnel action to reassign the employee to a Standard Position Description with a national security sensitivity level.
c. The manager must submit a written request to PS justifying the need for access to classified information or eligibility to hold a sensitive position.
d. The employee must complete a SF 86, *Questionnaire for National Security Positions*, and meet the necessary investigative criteria.
e. The required investigation must be initiated or upgraded to meet criteria for the sensitivity level.

Note: Conversely, if national security duties are no longer required, the position then reverts to a public trust risk designation.

10.23.1.3
(02-03-2020)
Position Sensitivity and Investigative Levels

(1) All national security positions must have a public trust risk designation in addition to a sensitivity designation. The sensitivity designation is complementary to the risk designation and could affect the investigative requirements. The position sensitivity and risk level designation must be based on an overall assessment of the damage that an individual, by virtue of the nature of the position, could cause to national security or the efficiency or integrity of the service.

a. A position at the Special Sensitive or Critical Sensitive level will automatically carry a risk designation at the **high risk** level.
b. A position at the Non-critical Sensitive level will automatically carry a risk designation at the **moderate risk** level, unless the IRS determines that the position should be designated at the high risk level.

(2) The Office of Personnel Management (OPM) Federal Investigative Standards establishes the level of investigation required for each position sensitivity designation for access to classified information or to hold a sensitive position. The standards consist of a five-tiered investigative model; Tier 3 and Tier 5 are the investigations conducted to determine eligibility for access to classified information or to hold a sensitive position.

a. Tier 3 investigation is conducted for positions designated as Non-critical Sensitive and/or requiring eligibility for access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information or assignment to a sensitive position.
b. Tier 5 investigation is conducted for positions designated Critical Sensitive, Special Sensitive and/or requiring access to Top Secret or Sensitive Compartmented Information (SC)I.

(3) The below chart shows the sensitivity and risk designation, investigative tier, form type and position sensitivity code for national security positions:

Sensitivity Designation	Risk Designation	Initial Investigation	Reinvestigation	SF Type	Sensitivity Code
Special Sensitive	High Risk	Tier 5	Tier 5R	SF 86	4N or 4C
Critical Sensitive	High Risk	Tier 5	Tier 5R	SF 86	3N or 3C
Non-Critical Sensitive	High Risk	Tier 5	Tier 5R	SF 86	2N or 2C
Non-Critical Sensitive	Moderate Risk	Tier 3	Tier 3R	SF 86	2N or 2C

Note: The alpha code associated with the sensitivity code:
N - Non Information Technology / Automated Information System related duties
C - Information Technology / Automated Information System related duties

10.23.1.4
(02-03-2020)
Investigations for National Security Positions

(1) The employment and retention of any employee in a national security position must be consistent with the interests of national security. At the IRS, that determination is related specifically to the individual's need for access to classified information, also referred to as a need for a security clearance, or eligibility to hold a sensitive position.

(2) Completion of a favorable background investigation does not in itself confer an employee's eligibility for access to classified information or to hold a sensitive position. An individual is eligible for access to classified information or to hold a sensitive position provided:

a. The individual has been determined to be eligible based on a completed and favorably adjudicated background investigation; and
b. It is determined that an individual requires access to classified information to perform official duties in a lawful and authorized government function, referred to as "need-to-know."

Note: The Associate Director, PS, not the prospective recipient, is responsible for determining if an employee's official duties require possession of, or access to, classified information and whether the employee has a "need-to-know."

(3) For an individual occupying a position designated "sensitive"(Non-critical Sensitive, Critical Sensitive, Special Sensitive), the position will be filled only by an individual for whom the requisite background investigation has been completed and favorably adjudicated prior to appointment.

(4) For an employee moving into a Critical Sensitive or Special Sensitive position, the investigation must be completed pre-appointment. Other than for Critical Sensitive or Special Sensitive levels, if the position risk or sensitivity of an incumbent's position is increased due to an accretion of duties and responsibilities, the incumbent may remain in the position, but the investigation

required by the higher risk/sensitivity level shall be initiated within 14 working days of the effective date of the new position designation.

(5) Requests for security clearances should be referred to PS. The instructions for submitting requests can be found at *Requesting a National Security Clearance*.

10.23.1.5
(02-03-2020)
Reciprocity of Background Investigations and National Security Adjudications

(1) PS will reciprocally accept background investigations, completed by an authorized investigative agency, that meet all or part of the investigative requirements and/or; national security eligibility adjudications, conducted by an authorized adjudicative agency, at the same or higher level, except as identified in paragraph 2 below.

a. In either case, PS may request the applicant/employee complete a SF 86C, *Standard Form 86 Certification,* to identify any changes since the last SF 86 submission and conduct the appropriate investigative inquiries related to the changes.
b. When a prior investigation meets part of the investigative requirements, PS will request the necessary investigative checks, through OPM, to bring the investigation up to standards for the type of investigation required for the position.

(2) Background investigations and national security eligibility adjudications **will not** be reciprocally accepted when:

a. New information has been reported, developed, or known to PS officials since the last investigation that indicates the individual no longer satisfies requirements to occupy a national security position;
b. The most recent background investigation is more than seven years old;
c. The most recent national security eligibility adjudication was granted with an exception, e.g., waiver, condition, deviation, or out of scope, for not meeting investigative or adjudicative standards;
d. The national security eligibility was granted on a temporary (interim), limited or one-time basis; or
e. The individual's national security eligibility is currently denied, revoked, or suspended.

(3) If background investigations and national security eligibility adjudications meet requirements for reciprocal acceptance, PS will not:

a. Request a new SF 86, *Questionnaire for National Security Positions*;
b. Review current background investigation, or the SF 86 upon which it was based; or
c. Initiate any new investigative checks.

Exception: PS will initiate the appropriate additional investigative checks if:

- The background investigation has not been adjudicated or does not meet standards for the type of investigation needed for the position; or
- PS requests a SF 86C from last SF 86 submission and the changed information warrants an investigative check(s).

10.23.1.6
(02-03-2020)
Reinvestigations for National Security Positions

(1) Employees with access to classified information or hold a sensitive position must undergo a periodic reinvestigation. Periodic reinvestigations are mandatory as circumstances change over time and may alter the eligibility of an employee's continued access to classified information or to hold a sensitive position.

a. Employees in a national security position who are eligible for access to classified information are reinvestigated accordingly:
   1. Critical Sensitive (Top Secret) or Special Sensitive (SCI), at least every five years.
   2. Non-Critical Sensitive (Secret), at least every ten years.
   3. Non-Critical Sensitive (Confidential), at least every 15 years.

b. Employees in a national security position who do not require access to classified information are reinvestigated at least once every five years.

Note: Employees who occupy a national security position can be reinvestigated if, at any time during the period of eligibility, there is reasonable cause that they no longer meet the standards to access classified information or hold a sensitive position.

10.23.1.7
(02-03-2020)
Continuous Evaluation

(1) Continuous Evaluation (CE) will be conducted on employees with eligibility to access classified information or hold a sensitive position. CE will consist of automated record checks to identify relevant information to determine if an employee can continue to occupy a national security position. The checks will include searches of commercial and US Government databases related to credit, criminal activity, suspicious financial activity, foreign travel, public records, and terrorism. CE can be conducted at any time during the period of national security eligibility.

10.23.1.8
(02-03-2020)
Reporting Personal and Foreign Activities

(1) All employees with eligibility to access classified information or hold a sensitive position must immediately report certain foreign and personal activities. This information must be reported to PS prior to participation in activities or otherwise immediately following the start of involvement. The reportable activities are illustrated below based on the level of access to classified information or position sensitivity.

Access to **Top Secret** or **SCI** or a **Critical or Special Sensitive** Position	Access to **Secret** or **Confidential** or a **Non-Critical Sensitive** Position
Unofficial foreign travel (30 days in advance)	Unofficial foreign travel (30 days in advance)
Unofficial foreign contacts (continuing association with a foreign national that involve bonds of affection, personal obligation, intimate contact, or exchange of personal information)	Unofficial foreign contacts (continuing association with a foreign national that involve bonds of affection, personal obligation, intimate contact, or exchange of personal information)
Direct involvement in foreign business	Application for/receipt of foreign citizenship

Foreign bank accounts / Ownership of foreign property	Application for, possession/use of foreign passport or identity card for travel
Application for/receipt of foreign citizenship	Attempted elicitation, exploitations, blackmail, coercion or enticement to obtain classified information
Application for, possession/use of foreign passport or identity card for travel	Media contact where media seeks access to classified information
Voting in a foreign election	Arrests
Adoption of non-U.S. citizen children	Bankruptcy or over 120 days delinquent on any debt
Attempted elicitation, exploitations, blackmail, coercion or enticement to obtain classified information	Alcohol/drug related treatment
Media contact where media seeks access to classified information	
Arrests	
Financial anomalies (bankruptcy, garnishment, over 120 days delinquent debt, unusual infusion of assets greater than $10,000 [inheritance, winnings, similar financial gain])	
Foreign national roommates (cooccupies a residence for a period of more than 30 calendar days)	
Cohabitation / Marriage	
Alcohol/drug related treatment	

(2) All personnel are responsible for immediately reporting, to PS, any adverse information known about other employees that may be of potential security or counterintelligence concern. The reportable actions by others are:

- Unwillingness to comply with rules or to cooperate with security requirements
- Unexplained affluence
- Alcohol abuse
- Illegal use or misuse of drugs or drug activity
- Criminal conduct
- Apparent or suspected mental health issues where there is reason to believe it may impact the individual's ability to protect classified or sensitive information

- Misuse of US Government property or information systems
- Any activity that raises doubts about an individual's continued national security eligibility

(3) All reportable information must be reported on the required form and submitted to PS. Failure to comply with reporting requirements may result in administrative action that includes, but is not limited to, revocation of national security eligibility. For additional guidance and forms, refer to *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*.

10.23.1.9
(02-03-2020)
Personnel Security Records

(1) PS must establish and maintain a personnel security file for all employees in a national security position. The file must include:

- Type and date of the investigation
- Results of the investigation
- Security and suitability adjudicative determinations
- National Security eligibility determinations
- Non-disclosure agreements
- Any significant personnel security/suitability information developed during employment

10.23.1.9.1
(02-03-2020)
Certificate of Clearance and/or Security Determination

(1) For employees granted access to classified information, a Treasury Department Form [TDF] 15-03.2, *Certificate of Clearance and/or Security Determination*, will be completed. This form documents the date and basis of the determination, but does not reflect any adverse information recorded in the personnel security file. When access to classified information has been granted, upgraded, administratively downgraded, suspended or cancelled, the following will occur:

a. The form will be issued and will include the level of access granted, and, where appropriate, whether the access was granted on an interim or final basis;
b. The Associate Director, PS, signs the form and the original signed certificate is mailed to the Official Personnel Folder (OPF) consolidation site;
c. The OPF office will file the original on the right side of the employee's OPF; and
d. A copy will be maintained in the employee's personnel security file.

10.23.1.9.2
(08-05-2016)
Classified Information Non-disclosure Agreement (SF 312)

(1) As a condition of being granted access to classified information, the individual must first undergo a security briefing. The briefing will be administered by a PS Security Officer or an officer acting on the authority of that office. The individual is informed of the obligations and responsibilities contingent upon being granted such access and must execute the SF 312, which must be appropriately witnessed per instructions in the SF 312 and returned to PS.

(2) For all IRS employees, the original SF 312 shall be placed on the right hand side of the OPF or retained in a file system of records that meets the Information Security Oversight Office's 50 year retention requirement.

10.23.1.9.3
(01-18-2008)
Written Consent Form for Access to Financial Records

(1) Every employee granted access to classified information must provide either Treasury or IRS with a written consent form. The consent form allows an authorized investigative agency access to financial and other records as defined in EO 12968 Section 1.2(e), *Access to Classified Information*, for the duration of the employee's access to classified information plus three years thereafter when any of the following occur:

a. There are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;
b. Treasury or a Treasury bureau has received credible information that an employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or
c. Circumstances indicate that the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

10.23.1.9.4
(08-05-2016)
Protection of Personnel Security Records

(1) Personally Identifiable Information (PII) in personnel security investigations, records and operations shall be carefully safeguarded to protect the interests of both the individual and the IRS pursuant to requirements of the Privacy Act of 1974 (Privacy Act). Unless classified at a higher level, personnel security information must be afforded the same degree of protection as material identified as Sensitive But Unclassified (SBU) and must be used only for authorized official purposes. When not in use, personnel security information must be stored in a locked container or compartment or in an equally secure area. For information on locked containers, see IRM 10.2.14.3.1, Locked Container.

(2) Personnel security investigation information requested by the subject of an investigation will be processed according to established procedures under provisions of the Privacy Act or the Freedom of Information Act (FOIA), as appropriate. Requests for the release of the results of any personnel security investigation should be referred to the Treasury/IRS or non-Treasury agency that conducted it. When another agency requests a copy of a PS report of investigation under the routine use provision of the Privacy Act (5 U.S.C. 552a), for the purpose of suitability or the granting of a security clearance, the request must be made in writing to:
IRS, Personnel Security
Attention: FOIA/PA Section
NCFB: Room C1-530
5000 Ellin Road
Lanham, MD 20706

(3) Reports containing classified information must be protected in accordance with EO 13526, *Classified National Security Information* and appropriate Treasury regulations.

10.23.1.10
(02-03-2020)
Prerequisites for Eligibility to Access Classified Information

(1) Employees will not be granted a security clearance for access to classified information unless they have:

- Been determined eligible for access based on a favorable adjudication of the requisite background investigation;
- Demonstrated a "need-to-know" the information to perform official duties;
- Signed a SF 312, *Classified Information Non-disclosure Agreement;* and
- Received contemporaneous training on the proper protection of classified information from unauthorized disclosure.

10.23.1.11
(02-03-2020)
Determining Eligibility for Access to Classified Information or to Hold a Sensitive Position

(1) A determination of eligibility for access to classified information or to hold a sensitive position is a discretionary security decision based on judgments by trained IRS adjudicators. The decision is based on eligibility standards set forth in SEAD 4, National Security Adjudicative Guidelines.

(2) Eligibility will be granted only where facts and circumstances indicate access to classified information or to hold a sensitive position is clearly consistent with the national security interests of the United States and any doubt will be resolved in favor of national security.

(3) Eligibility for access to classified information or to hold a sensitive position will be granted only to employees who are U.S. citizens (native born or naturalized) for whom an appropriate investigation has been completed by an appropriate government authority and favorably adjudicated.

10.23.1.11.1
(02-03-2020)
Possession of Foreign Passport

(1) Treasury/IRS employees with dual citizenship who possess a passport or any other identity type document issued by a foreign government raise a security concern that may be a disqualifying condition when considering an individual for access to classified information or eligibility to hold a sensitive position.

(2) To mitigate the security concern, employees **must** exit and enter the U.S. using a U.S passport while engaged in official and unofficial travel.

10.23.1.12
(02-03-2020)
Authority to Grant Access to Classified Information or Eligibility to Hold a Sensitive Position

(1) The Associate Director, PS, has the authority to make determinations of eligibility for access to classified information or to hold a sensitive position for IRS employees, and the consequent granting, suspending, denying and revoking access to classified information or eligibility to hold a sensitive position in accordance with provisions of EO 12968, EO 13467, 5 CFR 1400, SEAD 4 or any successor order.

(2) The Director, Office of Security Programs (OSP), Treasury retains the authority to determine the eligibility for access to classified information for the following IRS positions. This includes granting, denying, suspending, or revoking access to classified information.

- All IRS presidential appointees requiring confirmation by the Senate,
- Commissioner of IRS and Deputy Commissioners, and
- IRS personnel officers and any official with delegated authority to grant security clearances.

(3) The Director, OSP, as the official designee for the Assistant Secretary for Intelligence and Analysis as the Head of the Intelligence Community Element for Treasury, serves as the determination authority for eligibility for access to SCI for IRS employees.

10.23.1.13
(02-03-2020)
Limitations of Access Eligibility

(1) Treasury/IRS must keep the number of employees with access to classified information to the minimum necessary for the conduct of agency functions. Requesting or approving eligibility in excess of actual requirements is prohibited.

(2) The level of access granted will be limited to the classification level for which there is a need for access. Employees will not be granted access higher than needed to perform official duties.

(3) Access to classified information will not be requested or granted solely to permit entry to, or ease of movement within Treasury/IRS controlled areas when the employee has no need to access classified information.

(4) Employees will not be eligible merely by reasons of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or due to any particular title, rank, position, or affiliation.

10.23.1.14
(02-03-2020)
Interim Eligibility for Access to Classified Information

(1) Interim eligibility for access to classified information may be granted in **exceptional** circumstances when official functions must be performed prior to the completion of the final investigation. The access will be limited to the identified type(s) of classified information required to perform duties that were the basis for granting the interim access.

(2) If interim access is granted, the initial investigation must be expedited and the employee shall be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and the issuance of access eligibility approval.

(3) Interim access to Top Secret or SCI is not authorized by Treasury.

10.23.1.14.1
(02-03-2020)
Interim Access to Confidential or Secret Information

(1) Interim eligibility for access to Confidential or Secret access can be granted in **exceptional** circumstances under the following conditions:

1. Written justification by the cognizant supervisor, approved and signed by the requesting Business Unit's Head of Office to, and approved by, the Associate Director, PS;
2. A favorable review of a current SF 86;
3. The appropriate background investigation scheduled commensurate with the level of clearance; and
4. A favorable National Agency Check to include a Federal Bureau of Investigation fingerprint check.

10.23.1.15
(02-03-2020)
Mandatory Security Awareness Training for Access to Classified Information

(1) IRS employees who require access to classified information must receive an initial security orientation commensurate with the level of classification or sensitivity to which they have access. The training must be administered prior to the employee being granted a security clearance to access classified information. The success in protecting classified or sensitive information depends on the employee understanding:

- What needs to be protected;
- Why it needs to be protected;
- From whom to protect it; and
- How they must protect it.

(2) IRS employees must also receive annual refresher training to remind them of the security requirements for safeguarding classified information.

(3) Employees can refer to IRM 10.9.1, National Security Information, for additional guidance about safeguarding, storing, transporting and/or destroying classified information.

Note: Treasury's Special Security Office will conduct the initial and refresher training for IRS employees with access to SCI.

10.23.1.16
(02-03-2020)
Random Testing for Employees with Access to Classified Information

(1) National security positions designated as Non-Critical, Critical, or Special Sensitive, that require access to classified information at the Top Secret or Secret level, are identified as Testing Designated Positions (TDP) under the Drug-Free Workplace Program (DFWP). All Employees with an active Top Secret or Secret security clearance will be subjected to random drug testing. For more information, refer to *The IRS Drug-Free Workplace Program* or *The IRS Drug-Free Workplace Plan.*

10.23.1.17
(08-05-2016)
Protection of Whistleblowers with Access to Classified Information

(1) In accordance with the *Presidential Policy Directive 19,* effective October 12, 2012, employees eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information free of retaliation against them for reporting such actions. For more details, see *Treasury Security Manual TD P 15-71, Chapter 1, Section 8.*

10.23.1.18
(02-03-2020)
Security Clearance Verification

(1) When an IRS employee intends to visit a classified facility, and that facility requires verification of the employee's security clearance, the IRS PS office must certify that information to the host security office. Details regarding the proposed visit must be provided to PS five to seven business days in advance of the intended event to permit timely processing of the request. For instructions for requesting clearance verification, refer to *Clearance Verification*.

(2) PS will transmit the security clearance status and other required data, on the employee, to the host security office. The security clearance can only be certified for up to a one-year period. Acceptance of temporary or interim security clearances is at the discretion of the agency whose facility is to be visited.

(3) When a Federal employee is detailed to another agency, it is the responsibility of the parent agency to:

a. Ensure that the employee meets all investigative/clearance requirements for the new position, and
b. Grant any security clearance required for access to classified information.

(4) When employees of other Federal agencies or cleared contractor facilities require access to classified information at Treasury/IRS facilities, the sponsoring Treasury/IRS office must ask PS to obtain the pertinent security clearance verification data on the visitors.

a. For Federal employees, the verification data must come directly from the visitor's agency.
b. For contractors, verification must be obtained from the parent company or the Defense Industrial Security Clearance Office.

10.23.1.19
(02-03-2020)
Termination of Access to Classified Information

(1) Access to classified information must be administratively terminated when an employee no longer needs access to classified information. The employee's supervisor is responsible for notifying PS when the access is no longer required to perform official duties.

(2) For departing, transferring, or retiring employees, the debriefing should be administered before the employee's departure from the IRS. The employee's supervisor must notify PS two weeks prior to the employee's date of separation.

(3) Once access to classified information has been terminated, employees must:

a. Receive a security debriefing to emphasize the continuing responsibilities to protect classified information from unauthorized disclosure although their access has been terminated;
b. Sign the security debriefing acknowledgement section of the SF 312; and
c. Turn over all classified material and/or combinations or keys to any equipment storing classified information to their supervisor.

Note: Employees who no longer require access to SCI must receive a security debriefing from Treasury's SSO.

10.23.1.20
(02-03-2020)
Suspension of Access to Classified Information or Eligibility to Hold a Sensitive Position

(1) When adverse or unfavorable information becomes available concerning an employee with access to classified information or who holds a sensitive position, PS will immediately suspend the employee's access to classified or sensitive information. The suspension is temporary and the Associate Director, PS, must make a final decision to either re-instate or revoke the employee's access to classified information or eligibility to hold a sensitive position.

Note: For employees with access to SCI, when the collateral security clearance is suspended, PS will notify Treasury's SSO to suspend the employee's access to SCI.

(2) Access to classified or sensitive information **must** be suspended when an employee is:

a. Incarcerated due to a criminal conviction for a criminal offense; or
b. Absent without leave for a period exceeding 30 days

(3) Access to classified or sensitive information can be suspended in, but not limited to, the following situations:

a. Preparations are being made to revoke an employee's existing access to classified or sensitive information.
b. Additional time is needed to resolve adverse information that may require further investigation.
c. Pending removal and termination of employment resulting from a personnel action.
d. Employee's failure to submit required security forms or releases in the allotted time period.

10.23.1.20.1
(02-03-2020)
Notice of Suspension to the Employee

(1) Whenever a determination is made to suspend an employee's access to classified information or eligibility to hold a sensitive position, the following will occur:

a. The employee will be notified in writing of their suspended access to classified information or eligibility to hold a sensitive position by the Associate Director, PS, or a personnel security official, as appropriate;
b. The notification must include a brief statement of the reason(s) for the suspension, and a statement that the receipt of the notification is not an acknowledgement of culpability or concurrence with the suspension;
c. The notification must be delivered by personal delivery, government or commercial overnight courier or certified mail, within five calendar days from the date of the suspended access;
d. The employee must sign a receipt, acknowledging receipt of the notification. Regardless of whether delivery of the notice is refused or does not reach the individual through no fault of PS, suspension of access is immediate;
e. A copy of any notification required by this section shall be maintained in the employee's personnel security file; and
f. The suspension of access to classified or sensitive information remains in effect until an appropriate investigation is conducted and/or a final determination is made to revoke or reinstate the employee's access to classified or sensitive information by the Associate Director, PS. The employee will receive written notification of the final determination. If the final determination is to revoke access, the notification will include reasons for the decision. For employees with access to SCI, PS will notify Treasury's SSO of the final determination.

10.23.1.20.2
(02-03-2020)
Notice of Suspension to the Supervisor

(1) Upon the suspension of an employee's access to classified information or eligibility to hold a sensitive position, the Associate Director, PS, will notify the employee's supervisor in writing and the following will occur:

a. Associate Director, PS, and the employee's supervisor will take steps to ensure that the employee's name is removed from all local access rosters and notice of visit certifications. The supervisor must notify all employees (including contractors) working with the affected employee of the suspension to make certain the employee has no further access to classified or sensitive information. The cause of the suspension will not be disclosed to the supervisor or colleagues.
b. The employee's supervisor will ensure that the employee's government work space(s) does not contain unsecured classified or sensitive information during the period of the suspension of access to classified or sensitive information.
c. The employee's supervisor will ensure all combinations to classified storage containers, to which the employee had access, will be changed immediately unless sufficient controls exist to prevent the employee's continued access to the container.

10.23.1.21
(02-03-2020)
Denial or Revocation of Access to Classified Information or Eligibility to Hold a Sensitive Position

(1) The IRS will comply with Treasury's Security Manual, TD P 15-71, Chapter I, Section 6, *Denial or Revocation of Security Clearance* regarding denying or revoking an employee's access to classified information or eligibility to hold a sensitive position. The procedures do not apply to termination of access to classified information when the individual no longer has a "need-to-know".

(2) PS will proceed with access denial or revocation of eligibility for access to classified or to hold a sensitive position, as appropriate, when the Associate Director, PS, determines either of the following:

a. An individual who has been nominated for or currently has access to classified information or holds a sensitive position fails to meet applicable security criteria; or
b. There are insufficient mitigating factors that indicate whether national security eligibility fails to meet applicable security criteria.

(3) The Associate Director, PS , is the "Determining Official" for such determinations within the IRS.

(4) The IRS Human Capital Officer is the "Deciding Authority" for all such determinations within the IRS. For information about delegated authority, refer to: IRM 1.2.2.16.1 , Delegation Order 10-1, Performing Operating Functions Relating to Personnel Security.

(5) When access to classified information or eligibility to hold a sensitive position is denied or revoked, supervisors should contact their servicing Labor Relations Specialist to discuss options about the employee's employment status. Find your Labor Relations Specialists at: *Labor Relations Contact Guide*

10.23.1.21.1
(02-03-2020)
Notice of Determination

(1) As set forth in EO 12968, Section 5.2, the applicant or employee must be provided with a written Notice of Determination stating that they do not meet applicable eligibility standards for access to classified information. The written Notice of Determination must contain the following information:

a. A comprehensive and detailed explanation of the basis for the unfavorable national security eligibility determination;
b. The name and address of the official to whom the employee should direct any reply, request or other filing;
c. A copy of TD P 15-71, Chapter I, Section 6, *Denial or Revocation of Security Clearance* directing the individual to the description of the review proceedings; and
d. A copy of EO 12968, *Access to Classified Information*.

(2) When a Notice of Determination is issued, the following will occur:

- The notice must be delivered by personal delivery, certified mail, or government or commercial overnight courier within five (5) business days from the date of the determination notice. For types of mailing services used by the IRS, refer to: IRM 1.22.2, Mail and Transportation Management, United States Postal Service (USPS), Classes of Mail, USPS Additional Services and Small Package Carrier (SPC) Services.
- The applicant/employee must sign a receipt, acknowledging receipt of the notification.

- PS must maintain a copy of any notification required by this section in the applicant's/employee's personnel security file and provide a copy to the Director, OSP, Treasury.

Unless explicitly stated otherwise, the time period for a reply or other filing by an applicant/employee begins upon delivery of notification to the individual. Where delivery cannot be personally made or the delivery is refused, the time period begins five calendar days from the date the notice is mailed to the applicant/employee.

The due date specified for a reply or other filing by an applicant/employee is the date the reply or other filing must be received by the appropriate office. The reply or other filing can be made by personal delivery, facsimile, mail, or General Services Administration approved commercial overnight delivery.

10.23.1.21.2
(02-03-2020)
Review of Determination

(1) If an employee receives a notice of determination and requests a review of the determination, they may:

a. Be represented by counsel or other representative at their personal expense.
b. Request, in writing, not later than 15 calendar days after receipt of the notice of determination, either or both of the following:

1. Any documents, records, and reports upon which a denial or revocation is based, as defined in Section 5.2(a)(2) of EO 12968; or
2. The entire investigative file, as permitted by the national security standards and other applicable law.

c. Request, in writing, a review of the determination, by the IRS Human Capital Officer (the Deciding Authority), within the following time frames:

1. No later than 30 calendar days after receipt of the notice of determination, if no timely request has been made under paragraph (1) (b) above; or
2. No later than 30 calendar days after receipt of a notice from Treasury/IRS to the employee that the Treasury/IRS has made the final release of material requested, where a timely request under paragraph (1) (b) above has been made.

d. Request to appear personally before the IRS Human Capital Officer (the Deciding Authority) and present relevant documents, materials, and information. A request to appear personally must be made no later than 30 calendar days after the receipt of the Notice of Determination or receipt of a notice that IRS has released materials requested as described under paragraph (1) (c) above.

(2) Treasury/IRS must notify the employee when final release of documents or the file is made, so that the due date for a written reply may be set.

a. If the applicant or employee requests any documents, records or reports upon which a denial or revocation is based, the documents must be provided to the employee within 30 days of receipt of the request. The

documents must be provided to the extent they would be provided if requested and released under the FOIA or the Privacy Act, as applicable.

b. If the applicant or employee requests the entire investigative file, such documents must be provided promptly prior to the time set for a written reply, as permitted by the national security standards and other applicable law. A reply to the notice of determination must be reviewed by an official designated by Treasury/IRS officials or personnel security authority.

(3) A reply to the notice of determination must be reviewed by an official designated by a Treasury/IRS official or the IRS Deciding Authority. Upon completion of the review of the case, the Deciding Authority must notify the employee in writing of his or her decision (referred to as a Notice of Review).

a. The Notice of Review must be issued to the individual within five (5) business days of the final decision and delivered by personal delivery, certified mail , or government or commercial overnight courier.
b. The Notice of Review must state the reasons for the decision. If the decision of the Deciding Authority affirms the determination to deny or revoke access or eligibility, the notice of review must also inform the applicant/employee of the right to appeal the decision to the Treasury Security Appeals Panel, as described in EO 12968, Section 5.2(a)(6)(7).
c. The applicant/employee must sign a receipt, acknowledging receipt of the notification.
d. PS will maintain a copy of any notification required by this section in the applicant's/employee's personnel security file and provide a copy to the Director, OSP, Treasury.

10.23.1.21.3
(02-03-2020)
Appeal of Determination

(1) To file an appeal, the employee must submit a written appeal to the Treasury Security Appeals Panel within 30 days of receipt of the Notice of Review. An appeal filed beyond the 30-day time limit will not be accepted by the Treasury Security Appeals Panel unless the appellant demonstrates compelling reasons beyond his or her control that prevented timely filing.

The written appeal must include the following information:

a. Employee's full name, address and telephone number(s);
b. If applicable, the name, address and telephone number of the attorney or other representative;
c. A copy of Notice of Review; and
d. Any written statement, relevant documents, materials, or information the employee wants the Treasury Security Appeals Panel to consider.
e. The appeal should be addressed to:
Department of the Treasury
Treasury Security Appeals Panel
Annex 3180 / JBAB - Bldg 410/Door 123
250 Murray Lane SW
Washington, DC 20222

(2) When an applicant or employee requests a review of a Notice of Determination as described above in 10.23.1.21.2 or, after such review, they appeal to the Treasury Security Appeals Panel; the denial or revocation of eligibility for

access to classified information or to hold a sensitive position is implemented only when the appeal process is completed.

(3) Failure of the applicant or employee to take any of following actions will result in the termination of any further proceedings and the denial or revocation of access to classified information or to hold a sensitive position is upheld.

a. Request review of the determination,
b. Appeal to the Treasury Security Appeals Panel, or
c. Meet any applicable time limit for these actions.

(4) The Treasury Security Appeals Panel will review all documents related to the appeal case and make any necessary rulings on procedural matters.

(5) These provisions, consistent with EO 12968, Section 5.2(c), create no procedural or substantive rights.

Exhibit 10.23.1-1 (02-03-2020)
IRM 10.23.1 and IRM 10.23.3 Subsection Relocation Crosswalk

The chart below displays the relocation of subsections between IRM 10.23.1 and IRM 10.23.3.

Moved from IRM 10.23.1 to IRM 10.23.3	Moved to IRM 10.23.1 from IRM 10.23.3
10.23.1.2 Personnel Security Files	10.23.3.4 Position Sensitivity Risk Designation Levels - Paragraphs (7) (9) and (10)
10.23.1.3 Retention and Disposition of Investigative Reports	10.23.2.6 Investigations for National Security Clearances (Top Secret, Secret, and Confidential)
10.23.1.5 National Security or Suitability Adjudication of Background Investigations Conducted on Employees of PS and Human Capital Office Executive Team Members	
10.23.1.8 Transfer of Personnel Security Records and Clearances Between Treasury/Bureaus	

Exhibit 10.23.1-2 (02-03-2020)
IRM 10.23.1 Previous and Current Title and Subsection Crosswalk

The table below displays the IRM title change and the previous and current subsection numbering:

Previous Title	Current Title
IRM 10.23.1, Personnel Security	IRM 10.23.1, National Security Positions and Access to Classified Information
Previous Subsection Numbering	**Current Subsection Numbering**
10.23.1.1 Purpose	10.23.1.1 Program Scope and Objectives
10.23.1.2 Personnel Security Files	10.23.1.2 National Security Positions
10.23.1.3 Retention and Disposition of Investigative Reports	10.23.1.3 Position Sensitivity and Investigative Levels
10.23.1.4 Certificate of Clearance and/or Security Determination	10.23.1.4 Investigations for National Security Positions
10.23.1.5 National Security or Suitability Adjudication of Background Investigations Conducted on Employees of PS and Human Capital Office Executive Team Members	10.23.1.5 Reciprocity of Background Investigations and National Security Adjudications
10.23.1.6 Classified Information Nondisclosure Agreement (SF312)	10.23.1.6 Reinvestigations for National Security Positions
10.23.1.7 Written Consent Form for Access to Financial Records	10.23.1.7 Continuous Evaluation
10.23.1.8 Transfer of Personnel Security Records and Clearances Between Treasury/Bureaus	10.23.1.8 Reporting Personal and Foreign Activities
10.23.1.9 Protection of Personnel Security Records	10.23.1.9 Personnel Security Records
10.23.1.10 Monitoring Personnel, Security Clearance Changes and Adverse Information	10.23.1.10 Prerequisites for Eligibility to Access Classified or Sensitive Information
10.23.1.11 Clearance Verification	10.23.1.11 Determining Eligibility for Access to Classified Information or to Hold a Sensitive Position
10.23.1.12 Protection of Whistleblowers with Access to Classified Information	10.23.1.12 Authority to Grant Access to Classified Information or Eligibility to Hold a Sensitive Position
10.23.1.13 Determining Eligibility to Access Classified Information	10.23.1.13 Limitations of Access Eligibility
10.23.1.14 Suspension of Access to Classified Information	10.23.1.14 Interim Eligibility for Access to Classified Information
10.23.1.15 Denial and Revocation of Security Clearance	10.23.1.15 Mandatory Security Awareness Training for Access to Classified Information

Exhibit 10.23.1-2 (Cont. 1) (02-03-2020)
IRM 10.23.1 Previous and Current Title and Subsection Crosswalk

	10.23.1.16 Random Testing for Employees with Access to Classified Information
	10.23.1.17 Protection of Whistleblowers with Access to Classified Information
	10.23.1.18 Security Clearance Verification
	10.23.1.19 Termination of Access to Classified Information
	10.23.1.20 Suspension of Access to Classified Information or Eligibility to Hold a Sensitive Position
	10.21.1.21 Denial or Revocation of Access to Classified Information or Eligibility to Hold a Sensitive Position