



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.23.1

DECEMBER 18, 2024

## EFFECTIVE DATE

(12-18-2024)

## PURPOSE

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

## MATERIAL CHANGES

- (1) IRM 10.23.1.1 - Internal controls added or updated in compliance with IRM 1.11.2, Internal Revenue Manual Process. Included information related to the program background, program owner, authority, roles/responsibilities, program management and review, program controls, acronyms, security terms/definitions and related resources.
- (2) IRM 10.23.1.6 - Guidance on Continuous Vetting (CV) was added outlining the new policy and requirements under the CV process.
- (3) IRM 10.23.1.6 Reinvestigations for National Security Positions was removed.
- (4) IRM 10.23.1.7 Continuous Evaluation was removed.
- (5) IRM 10.23.1.8.2 was updated to include the new policy on digital signatures on an SF 312 Nondisclosure Agreement.

## EFFECT ON OTHER DOCUMENTS

IRM 10.23.1, **National Security Positions and Access to Classified Information**, dated February 3, 2020, is superseded.

This IRM incorporates Interim Guidance Memorandum HCO-06-0623-0008, Continuous Vetting for National Security, Public Trust, and Sensitive positions in the IRS, dated September 25, 2023.

## AUDIENCE

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

Traci M. DiMartini  
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 Background

10.23.1.1.2 Authority

10.23.1.1.3 Roles and Responsibilities

10.23.1.1.4 Program Management and Review

10.23.1.1.5 Program Controls

10.23.1.1.6 Commonly Used Acronyms

10.23.1.1.7 Security Terms and Definitions

10.23.1.1.8 Related Resources

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 Continuous Vetting

10.23.1.7 Reporting Personal and Foreign Activities

10.23.1.8 Personnel Security Records

10.23.1.8.1 Certificate of Clearance and/or Security Determination

10.23.1.8.2 Classified Information Non-Disclosure Agreement (SF 312)

10.23.1.8.3 Written Consent Form for Access to Financial Records

10.23.1.8.4 Protection of Personnel Security Records

10.23.1.9 Prerequisites for Eligibility to Access Classified Information

10.23.1.10 Determining Eligibility for Access to Classified Information or to Hold a Sensitive Position

10.23.1.10.1 Possession of Foreign Passport

10.23.1.11 Authority to Grant Access to Classified Information or Eligibility to Hold a Sensitive Position

10.23.1.12 Limitations of Access Eligibility

10.23.1.13 Interim Eligibility for Access to Classified Information

10.23.1.13.1 Interim Access to Confidential or Secret Information

10.23.1.14 Mandatory Security Awareness Training for Access to Classified Information

10.23.1.15 Random Testing for Employees with Access to Classified Information

10.23.1.16 Protection of Whistleblowers with Access to Classified Information

10.23.1.17 Security Clearance Verification

10.23.1.18 Termination of Access to Classified Information

10.23.1.19 Suspension of Access to Classified Information or Eligibility to Hold a Sensitive Position

10.23.1.19.1 Notice of Suspension to the Employee

- 
- 10.23.1.19.2 Notice of Suspension to the Supervisor
  - 10.23.1.20 Denial or Revocation of Access to Classified Information or Eligibility to Hold a Sensitive Position
    - 10.23.1.20.1 Notice of Determination
    - 10.23.1.20.2 Review of Determination
    - 10.23.1.20.3 Appeal of Determination

Exhibits

- 10.23.1-1 Security Terms and Definitions

10.23.1.1  
(12-18-2024)  
**Program Scope and Objectives**

- (1) **Purpose.** This section establishes general policy and procedures for national security position requirements, retention and protection of personnel security records. It also establishes national security eligibility for access to classified information or holding a public trust or sensitive position. The Associate Director, Personnel Security Office (PS) will maintain personnel security operations in accordance with the procedures outlined herein.
- (2) **Audience.** Unless otherwise indicated, the policies, authorities, procedures, and instructions contained in this IRM apply to all business units. Bargaining unit employees should review negotiated agreement provisions relating to subjects in the IRM. Should any of these instructions conflict with provisions in the negotiated agreement, the agreement prevails.
- (3) **Policy Owner.** Human Capital Office, Policy Office
- (4) **Program Owner.** Human Capital Office (HCO)
- (5) **Primary Stakeholder.** HCO, OHRO, TA, PS, and Strategic Recruitment & Hiring Services
- (6) **Contact Information.** Personnel Security at:  
*Personnel Security Contacts*

10.23.1.1.1  
(12-18-2024)  
**Background**

- (1) This IRM is part of the Servicewide effort to transform the federal personnel vetting process to incorporate the minimum standards of continuous vetting (CV).
- (2) The CV process leverages a risk-managed approach of seven automated record checks that are conducted in real-time.

10.23.1.1.2  
(12-18-2024)  
**Authority**

- (1) This IRM supplements policies and requirements and must be read in conjunction with cited authorities.
- (2) **Statutes:** United States Code (USC) at: <http://uscode.house.gov/browse.xhtml>
  - a. 3 USC Chapter 2, Sections 105, 106 and 107 at: [https://uscode.house.gov/view.xhtml?req=\(title:3%20chapter:2%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:3%20chapter:2%20edition:prelim))
  - b. 5 USC 11001: Enhanced personnel security programs at: [https://uscode.house.gov/view.xhtml?req=\(title:5%20section:11001%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:5%20section:11001%20edition:prelim))
  - c. 50 USC Chapter 45, Security Clearance and Classified Information at: [https://uscode.house.gov/view.xhtml?req=\(title:50%20chapter:45%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:50%20chapter:45%20edition:prelim))
- (3) **Regulations:** Code of Federal Regulations (CFR) at: <https://www.ecfr.gov/>
  - a. 5 CFR 1400.201, Sensitivity level designations and investigative requirements at: <https://www.ecfr.gov/current/title-5/chapter-IV/part-1400/subpart-B/section-1400.201>
  - b. 5 CFR 732, National Security Positions at: <https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-732>
  - c. 32 CFR Chapter XX, Information Security Oversight Office, National Archives and Records Administrations at: <https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX>
- (4) **Federal Register (FR):** <https://www.federalregister.gov/>

- a. 75 FR 51609 (EO 13549), Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities at: <https://www.federalregister.gov/documents/2010/08/23/2010-21016/classified-national-security-information-program-for-state-local-tribal-and-private-sector-entities>
- b. 87 FR 17951, Classified National Security Information at: <https://www.federalregister.gov/documents/2022/03/29/2022-06548/classified-national-security-information>
- c. 88 FR 6192 Suitability and Fitness Vetting at: <https://www.federalregister.gov/documents/search?conditions%5Bterm%5D=2023-01650>
- d. Executive Order (EO) 13764, Amending the Civil Service Rules, EO 13488, and EO 13467 at: <https://www.federalregister.gov/documents/2017/01/23/2017-01623/amending-the-civil-service-rules-executive-order-13488-and-executive-order-13467-to-modernize-the>
- e. EO 12968, Access to Classified Information at: <https://www.federalregister.gov/documents/1995/08/07/95-19654/access-to-classified-information>

(5) **Other:**

- a. Office of the Director of National Intelligence, Security Executive Agent Directive (SEAD) 3, 4, 6 and 7 at: <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy>
- b. Presidential Policy Directive 19 at: <https://www.dni.gov/files/ICIG/Documents/Policy/Whistleblowing/PPD-19.pdf>
- c. Digital Signature on the Standard Form (SF) 312, Classified Information Nondisclosure Agreement at: <https://isoo-overview.blogs.archives.gov/2022/05/11/digital-signatures-on-the-standard-form-sf-312-classified-information-nondisclosure-agreement/>
- d. National Agreement between IRS and National Treasury Employees Union (NTEU) at: <https://publish.no.irs.gov/cat12.cgi?request=CAT1&catnum=32781>

10.23.1.1.3  
(12-18-2024)  
**Roles and  
Responsibilities**

- (1) The Associate Director of PS has the responsibility for adjudication of background investigations for IRS applicants/employees who occupy national security, public trust, or sensitive positions.
- (2) The Associate Director of PS is the deciding authority responsible for reviewing any reply from the applicant/employee when eligibility to occupy a national security, public trust, or sensitive position is denied or revoked.
- (3) The Department of the Treasury, Treasury Security Appeals, is responsible for resolving the eligibility decision if the applicant appeals the decision to deny or revoke eligibility to occupy a national security position.

10.23.1.1.4  
(12-18-2024)  
**Program Management  
and Review**

- (1) The HCO, OHRO, TA, PS office oversees program management and reviews relating to personnel security matters.

10.23.1.1.5  
(12-18-2024)  
**Program Controls**

- (1) Program controls are outlined in IRM 6.10.1, IRS Personnel Staffing Accountability, for program oversight requirements.

10.23.1.1.6  
(12-18-2024)  
**Commonly Used  
Acronyms**

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

Acronyms	Definitions
CE	Continuous Evaluation
CFR	Code of Federal Regulations
CI	Counterintelligence
CV	Continuous Vetting
CVS	Central Verification System
EO	Executive Order
FOIA/PA	Freedom of Information Act/ Privacy Act
NCIC	National Crime Information Center
NDA	Non-Disclosure Agreement
NLETS	National Law Enforcement Tele- communications System
OPF	Official Personnel File
OSP	Office of Security Programs (Treasury)
PS	Personnel Security
SCI	Sensitive Compartmented Infor- mation
SEAD	Security Executive Agent Directive
SF	Standard Form
SSO	Special Security Office (Treasury)
TDP	Treasury Directive Publication

10.23.1.1.7  
(12-18-2024)  
**Security Terms and  
Definitions**

- (1) A list of security terms and definitions can be found at, Exhibit 10.23.1-1, Security Terms and Definitions.

10.23.1.1.8  
(12-18-2024)  
**Related Resources**

- (1) Information Security Oversight Office (ISOO), Digital Signatures on the Standard Form (SF) 312, Classified Information Nondisclosure Agreement at: <https://isoo-overview.blogs.archives.gov/2022/05/11/digital-signatures-on-the-standard-form-sf-312-classified-information-nondisclosure-agreement/>

- (2) United States Department of the Treasury, Treasury Directive 15-71 at: <https://home.treasury.gov/about/general-information/orders-and-directives/treasury-directive-15-71>
- (3) IRM 10.9.1, National Security Information Classified National Security Information at: <http://irm.web.irs.gov/Part10/Chapter9/Section1/IRM10.9.1.aspx>

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 those with duties related to:
  - Protecting the nation, its citizens, and residents from acts of terrorism, espionage, or foreign aggression;
  - Law Enforcement, public safety, or criminal justice;
  - Protecting or controlling access to facilities or information systems; and
  - Investigating or adjudicating 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 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 an 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 both public trust risk designation and 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's sensitivity designation for accessing classified information or holding 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 accessing classified information or holding 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 (SCI).
- (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 effectuating the personnel action.
- (4) For an employee moving into a Critical Sensitive or Special Sensitive position, the investigation must be completed pre-appointment. For all other positions, 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) The PS office 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 *Standard Form 86 Certification*, (SF 86C) 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 does not meet all of the IRS 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 become 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 an 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
- The PS office requests an SF 86C from the last SF 86 submission and the changed information warrants an investigative check(s).

## 10.23.1.6 (12-18-2024) Continuous Vetting

- (1) The CV must be conducted on covered individuals who require continued eligibility to access classified information or hold a public trust or sensitive position.
- (2) The CV process will include automated records checks (ARC) that are conducted to identify adjudicative relevant information for assessing the continued eligibility of a covered individual at any time during the period of eligibility. The ARC will include checks of commercial databases, U.S. Government (USG) databases, and other information lawfully available to security officials at any time during the period of eligibility. Below is a chart identifying the checks, data sources and minimum frequency required for the CV process.

**Note:** Enrollment in the Federal Bureau of Investigations (FBI) subscription-based Rap Back program requires the covered individual be notified of enrollment in writing making them aware of the present and potential use of their fingerprints presented with the FBI Privacy Act Notice and Noncriminal Justice Applicant's Privacy Rights.

Check	Data Source	Minimum Frequency
Eligibility	DISS, CVS, or successor repository of records	Daily
Terrorism	Terrorist Identities Datamart Environment	Daily
	FBI NCIC person file for Known or Suspected Terrorist	Daily
	FBI Name Check (FBI-NNCP)	Risk-based, but not less frequent than once every five years

Check	Data Source	Minimum Frequency
Criminal Activity	FBI NCIC Person Files	Daily
	FBI's Next Generation Identification Rap Back	Daily
	NLETS and State repositories	Quarterly
	Local Laws	Risk-based, but not less frequent than once every five years for localities not already covered by NLETS/ statewide searches where DCSA has validated the sufficiency of the check
Foreign Travel	Department of Homeland Security (DHS) Advanced Passenger Inquiry System	Daily, but review required only when CI, insider threat, or other issues are present
	DHS Border Crossing Information	
Suspicious Financial Activity	The Department of the Treasury Financial Crimes Enforcement Network	Monthly
Credit Bureau Checks	Commercial Provider(s)	Yearly
Public Records Check (Judgments, liens, bankruptcies, etc.)	Commercial Provider(s)	Quarterly

- (3) The CV process must protect the privacy, civil liberties, and personally identifiable information of covered individuals and any other individual whose information is inadvertently collected as part of the CV process. Absent a national security concern, criminal reporting requirements, or other legal requirements, information pertaining to individuals other than the covered individual will not be retained unless that information is relevant to a security determination of the covered individual.
- (4) The CV process will make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual.
- (5) The CV process will ensure investigations conducted are consistent with the Federal Investigation Standards.

- (6) The CV process will ensure covered individuals are aware of the CV requirements as an element of the Personnel Security Program and their continuing security and CI reporting obligations. The CV policy and requirements will be included in initial and annual security awareness training.
- (7) The PS Office will act on and share relevant information that may result in an adverse determination of a covered individual's continued national security eligibility with the appropriate security, CI, and/or insider threat working groups that have a direct interest in the covered individual.
- (8) The CV will cease on individuals who no longer meet the definition of covered individual (for example, termination of employment, no longer affiliated with the USG).

10.23.1.7  
(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, but no later than immediately following the start of involvement, in reportable activities. The types of reportable activities are based on the level of access to classified information or position sensitivity, as illustrated below:

<b>Access to Top Secret or SCI Information or a Critical or Special Sensitive Position</b>	<b>Access to Secret or Confidential Information or a Non-Critical Sensitive Position</b>
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)
Application for/receipt of foreign citizenship	Application for/receipt of foreign citizenship
Application for, possession/use of foreign passport or identity card for travel	Application for, possession/use of foreign passport or identity card for travel
Attempted elicitation, exploitations, blackmail, coercion or enticement to obtain classified information	Attempted elicitation, exploitations, blackmail, coercion or enticement to obtain classified information
Media contact where media seeks access to classified information	Media contact where media seeks access to classified information
Arrests	Arrests
Adoption of non-U.S. citizen children	Bankruptcy or over 120 days delinquent on any debt

<b>Access to Top Secret or SCI Information or a Critical or Special Sensitive Position</b>	<b>Access to Secret or Confidential Information or a Non-Critical Sensitive Position</b>
Alcohol/drug related treatment	Alcohol/drug related treatment
Foreign bank accounts/Ownership of foreign property	
Voting in a foreign election	
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 (co-occupies a residence for a period of more than 30 calendar days)	
Cohabitation/Marriage	
Direct involvement in foreign business	

- (2) All employees are responsible for immediately reporting to PS any adverse information known about other employees that may be of a potential security or CI 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; and
  - 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 All Employees Who have Access to Classified Information or Who Hold a Sensitive Position*.

10.23.1.8  
(02-03-2020)  
**Personnel Security  
Records**

- (1) The 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; and
  - Any significant personnel security/suitability information developed during employment.

10.23.1.8.1  
(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 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, will sign the form and mail the original signed certificate 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.

10.23.1.8.2  
(12-18-2024)  
**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 an SF 312, **Classified Information Nondisclosure Agreement**, which must be appropriately witnessed per instructions on the SF 312 and returned to PS.
- (2) When executing an SF 312, only digital signatures created using a Personal Identity Verification (PIV) card or the common access card issued by the U.S. Government that is compliant with Homeland Security Presidential Directive 12, will be accepted. No other digital signature is authorized for use.
- (3) When an SF 312 is digitally signed, it is not required that a witness observe and verify the digital signature, or that an official subsequently accept the signature. When an SF 312 is signed using "wet ink" signature, a witness must observe and verify the signature, and an official must subsequently accept the signature.
- (4) For all IRS employees, the original SF 312 will 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.



10.23.1.8.3  
(01-18-2008)

**Written Consent Form  
for Access to Financial  
Records**

- (1) Every employee granted access to classified information must provide either Treasury or the 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.

10.23.1.8.4  
(12-18-2024)

**Protection of Personnel  
Security Records**

- (1) Pursuant to the requirements of the Privacy Act of 1974, Personally Identifiable Information (PII) in personnel security investigations, records and operations must be carefully safeguarded to protect the interests of both the individual and the IRS. 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, refer to IRM 10.2.14.3.3, Locked Containers.
- (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.
- (4) The loss, theft, or inadvertent unauthorized disclosure of PII in personnel security investigations, records, and operations must be reported immediately upon discovery to the Office of Privacy, Governmental Liaison and Disclosure (PGLD) Incident Management Office using PGLD's PII Breach Reporting Form. For additional information and reporting guidance, refer to IRM 10.5.4, Privacy



and Information Protection, Incident Management Program, and the Report losses Theft or Disclosures page in the Disclosure and Privacy Knowledge Base site.

10.23.1.9  
(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” of the information to perform official duties;
  - Signed an SF 312, *Classified Information Non-Disclosure Agreement*; and
  - Received contemporaneous training on the proper protection of classified information from unauthorized disclosure.

10.23.1.10  
(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.

10.23.1.10.1  
(02-03-2020)  
**Possession of Foreign Passport**

- (1) Treasury/IRS employees with dual citizenship who possess a passport or any other identity 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.

10.23.1.11  
(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 the IRS and Deputy Commissioners, and
- The 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.

10.23.1.12  
(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.

10.23.1.13  
(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 will 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.

10.23.1.13.1  
(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.

10.23.1.14  
(02-03-2020)

## **Mandatory Security Awareness Training for Access to Classified Information**

- (1) The IRS employee who requires 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's understanding of:
  - What needs to be protected;
  - Why it needs to be protected;
  - From whom to protect it; and
  - How they must protect it.
- (2) All IRS employees must receive annual refresher training to remind them of the security requirements for safeguarding classified information.
- (3) The IRS employees can refer to *IRM 10.9.1* Classified 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.

10.23.1.15  
(12-18-2024)

## **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*.

10.23.1.16  
(12-18-2024)

## **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*.

10.23.1.17  
(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) The PS office will transmit the security clearance status and other required data about 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.

10.23.1.18  
(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, a debriefing must be administered by PS or the manager before the employee's departure. 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 an 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 Security Service Office (SSO).

10.23.1.19  
(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.

10.23.1.19.1  
(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 must 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 Security Service Office of the final determination.

10.23.1.19.2  
(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 immediately notify the employee's supervisor in writing and the following must occur:
- a. The 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 will 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 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.

10.23.1.20  
(12-18-2024)

**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 the termination of access to classified information when the individual no longer has a "need-to-know".
- (2) The PS office 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 such determinations within the IRS. For information about delegated authority, refer to IRM 1.2.2.11.1, 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/Employee Relations & Negotiations (LERN) office to discuss options about the employee's employment status. Find your labor relations specialists at: *LERN Service Delivery*

10.23.1.20.1  
(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 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.
- The PS office 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 was 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.

10.23.1.20.2  
(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, no 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 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 the IRS has released materials requested as described under paragraph (1) (c) above.

- (2) The 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 calendar 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 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. The PS office 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.

10.23.1.20.3  
(12-18-2024)

#### **Appeal of Determination**

- (1) To file an appeal, the employee must submit a written appeal to the Treasury Security Appeals Panel within 30 calendar days of receipt of the Notice of Review. An appeal filed beyond this time limit will not be accepted by the Treasury Security Appeals Panel unless the appellant demonstrates compelling reasons beyond their 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 the 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 10.23.1.20.1 or, after such review, they can 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.

**This Page Intentionally Left Blank**

**Exhibit 10.23.1-1 (12-18-2024)**  
**Security Terms and Definitions**

Terms	Definitions
Adjudication	The evaluation of information in an individual's background investigation or any other relevant/reliable information to determine if an individual is suitable or fit to perform work for or on behalf of the federal government, eligible for logical or physical access, or eligible to hold a sensitive position. An adjudicator carefully weighs information gathered during the background investigation (favorable-unfavorable, past-present) to reach a final determination.
Adjudicator	A trained personnel security specialist who evaluates background investigations and other pertinent information to make employment suitability and national security eligibility determinations.
Adverse Information	Information that adversely reflects on a person's character, integrity or reliability that suggests that their ability to safeguard sensitive information may be impaired, or that their employment and national security eligibility is not in the best interest of the IRS. For example, a history of misbehavior, etc., drug abuse, criminal activity, employment misconduct, etc.
Background Investigation	An official examination of facts or other pertinent information that covers a defined period of normally no more than 10 years. The information is compiled from a review of various records, interview with the subject, and interviews with persons who have knowledge of the subject. The information collected must be sufficient to allow an affirmative or negative determination of a person's eligibility and suitability to work for the federal government.
Central Verification System (CVS)	A system operated by the OPM that contains information on security clearances, investigations, suitability, fitness determinations, HSPD-12 decisions, PIV credentials, and polygraph data.
Continuous Evaluation (CE)	A vetting process to review the background of an individual who has been determined to be eligible for access to classified NSI or to hold a sensitive position at any time during the period of eligibility.
Continuous Vetting (CV)	Refers to the process of reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.

**Exhibit 10.23.1-1 (Cont. 1) (12-18-2024)**  
**Security Terms and Definitions**

Terms	Definitions
Covered Individuals	<ul style="list-style-type: none"> <li>• A person who performs work for or on behalf of the executive branch or who seeks to perform work for or on behalf of the executive branch but does not include the President or employees for the President under 3 USC Section 105 or 107, the Vice President under 3 USC Section 106 or annual legislative branch appropriations acts.</li> <li>• A person who performs work for or on behalf of a state, local, tribal or private sector entity, as defined in EO 13549, but does not include duly elected or appointed Governors of a State or territory, or an official who has succeeded to that office under applicable law.</li> <li>• A person working in or for the legislative or judicial branches with eligibility for access to classified information and the investigation or determination was conducted by the executive branch, but does not include Members of Congress, Justices of the Supreme Court, and Federal judges appointed by the President.</li> <li>• Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who require eligibility for access to classified information or eligibility to hold a sensitive position, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.</li> </ul>
Credit Check	A credit history report conducted on the subject of a background investigation. The report contains financial information collected from creditors, lenders, and public records and organized by credit bureaus or other credit reporting services.
Fingerprint Check	Also referred to as a criminal history record or rap sheet – Is a listing of specific information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, federal employment, naturalization, or military service.
Foreign National	An individual who is not a U.S. citizen or a LPR authorized to reside in the U.S.
High Risk Position	A public trust position that has the potential for exceptionally serious impact on the “efficiency of the service” involving duties especially critical to the agency or a program mission with broad scope of policy or program authority.
Interim Staff-like Access	Access granted on a temporary basis based on the completion of minimum investigative requirements pending the completion of full investigative requirements, including receipt and adjudication of the individual’s completed background investigation.
Low Risk Position	Positions involving duties that have the potential for limited impact upon the agency mission based upon their limited program responsibilities that affect the “efficiency of the service”.

**Exhibit 10.23.1-1 (Cont. 2) (12-18-2024)**  
**Security Terms and Definitions**

Terms	Definitions
Moderate Risk Position	A public trust position involving duties having the potential for moderate to serious impact on an agency or a program mission with significant program responsibilities and delivery of customer services to the public.
National Security Positions	Any position, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on national security. Such positions include, but not limited to, those requiring eligibility to classified NSI; protecting the nation from acts of terrorism, espionage, or foreign aggression; and developing plans or policies related to national defense/military operations. Refer to 5 CFR 1400, Designation of National Security Positions, Section 1400.102.
Nondisclosure Agreement (NDA)	A legally binding contract executed by an individual to protect U.S. Government sensitive and/or classified NSI from unauthorized disclosure. The agreement is a condition to have access to sensitive/ classified NSI and specifies the security requirements and penalties for noncompliance. For access to classified NSI, the Classified Non-disclosure Agreement SF 312 is required.
Notification of Access	A written notice delivered to the COR and contractor employee that signifies the final staff-like access determination.
Personally Identifiable Information (PII)	Also considered SBU information. Information that is linked or linkable to an individual that must be protected to prevent the possibility of identity theft or invasion of privacy.
Personnel Security (PS)	An organization comprised of security specialists that are engaged in the formulation and application of security policies and procedures involving the trustworthiness and loyalty of persons employed with the federal government in sensitive and non-sensitive positions.
Position Sensitivity	A risk designation based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a position, could have an effect on the “efficiency of the service”.
Public Trust Position	Positions at the high or moderate risk levels as determined by the position’s potential for adverse impact to the “efficiency of the service”. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities or other duties demanding a significant degree of public trust, and positions involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain.

**Exhibit 10.23.1-1 (Cont. 3) (12-18-2024)**  
**Security Terms and Definitions**

<b>Terms</b>	<b>Definitions</b>
Rap Back	A subscription-based program offered by the FBI. Rap Back provides for an ongoing ability to gather real time information about an individual's behavior using classifiable fingerprints provided by the subscribing agency and continuously comparing those fingerprints with new criminal history and civil records provided to the FBI by State Identification Bureaus.
Reasonably Exhaustive Efforts	The appropriate level of effort to resolve issues or corroborate discrepant information. They may include multiple attempts or techniques to satisfy the issue, attempts to corroborate the activity through references from the background investigation, and/or attempts to obtain and pursue additional leads through other aspects of the investigation.
Reciprocity	Recognition and acceptance of prior background investigations and favorable fitness determinations conducted by another federal agency, without further processing when the determination was based on equivalent criteria used by gaining agency, i.e., investigation meets or exceeds required position risk/sensitivity level, investigation completed within the last five years.
Security Clearance	Certification issued by a designated personnel security official or designee that grants an individual access to classified NSI, on a need-to-know basis, up to the required classification level (Top Secret, Secret, or Confidential) to perform official duties.
Sensitive But Unclassified Information (SBU)	Any sensitive information (including tax and tax-related information) that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Sensitive Position	Positions that the occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified NSI.