



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.23.3

AUGUST 5, 2025

## EFFECTIVE DATE

(08-05-2025)

## PURPOSE

- (1) This transmits revised IRM 10.23.3, *Personnel Security, Personnel Security Operations*.

## MATERIAL CHANGES

- (1) Updated IRM section title from Suitability for Employment and Personnel Security Operations to Personnel Security Operations.
- (2) IRM 10.23.3.1, Program Scope and Objectives, has been updated to reflect current program controls.
- (3) IRM 10.23.3.2, Applicant Suitability Pre-screening and Fingerprint Check, was moved to 6.731.1.2.
- (4) IRM 10.23.3.3, Credit Checks, was moved to 6.731.1.5.
- (5) IRM 10.23.3.4, Scope of Position Designation System, was moved to 6.731.1.3.
- (6) IRM 10.23.3.4.1, Position Risk Level Determination, was moved to 6.731.1.3.1.
- (7) IRM 10.23.3.5, Investigation Requirements, was moved to 6.731.1.4.
- (8) IRM 10.23.3.6, Investigation Tiers, was moved to 6.731.1.4.1.
- (9) IRM 10.23.3.7, Position Risk Level for IT Privileged Access, was moved to 6.731.1.3.2.
- (10) IRM 10.23.3.8, Reinvestigation Requirements, was moved to 6.731.1.4.4.
- (11) IRM 10.23.3.9, Suitability Investigations, was moved to 6.731.1.7.
- (12) IRM 10.23.3.10 (2), Personnel Security Responsibilities, was moved to 6.731.1.1.3 (4).
- (13) IRM 10.23.3.10.1, Suitability Adjudication, was moved to 6.731.1.1.7.4.
- (14) IRM 10.23.3.11, Office of Personnel Management Roles/Responsibilities, was moved to 6.731.1.3 (4).
- (15) IRM 10.23.3.12, National Background Investigations Bureau Roles/Responsibilities, was moved to 6.731.1.1.3 (5).
- (16) IRM 10.23.3.13, Debarment Policy and Delegation of Authority, was moved to 6.731.1.8.
- (17) IRM 10.23.3.13.1, Imposing IRS Debarment - IRS Deciding Official, was moved to 6.731.1.8.1.
- (18) IRM 10.23.3.13.2, Debarment Cases Referred to OPM by IRS, was moved to 6.731.1.8.2.
- (19) IRM 10.23.3.13.3, Debarment Based on Suitability Determination, was moved to 6.731.1.8.3.
- (20) IRM 10.23.3.13.4, Timing of Suitability Determinations, was moved to 6.731.1.7.2.
- (21) IRM 10.23.3.13.5, Administrative Procedures, was moved to 6.731.1.8.4.
- (22) IRM 10.23.3.16, Criteria for Making Suitability Determination, was moved to 6.731.1.7.4 (2).
- (23) IRM 10.23.3.17, Suitability Due Process, was moved to 6.731.1.7.5.

- (24) IRM 10.23.3.18, Appeal Rights, was moved to 6.731.1.7.6.
- (25) Exhibit 10.23.3-1 was removed.
- (26) Exhibit 10.23.3-2 was removed.

#### **EFFECT ON OTHER DOCUMENTS**

IRM 10.23.3, Personnel Security (PS), Personnel Security/Suitability Program, dated May 9, 2019, is superseded. Portions of IRM 10.23.3, dated May 9, 2019, were moved to IRM 6.731.1 Suitability Determinations for Employment. This IRM incorporates portions of 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 business units

Max R. Wyche  
acting IRS Human Capital Officer

---

10.23.3

Personnel Security Operations

## Table of Contents

10.23.3.1 Program Scope and Objectives

10.23.3.1.1 Background

10.23.3.1.2 Authorities

10.23.3.1.3 Roles and Responsibilities

10.23.3.1.4 Program Management and Review

10.23.3.1.5 Program Controls

10.23.3.1.6 Commonly Used Acronyms

10.23.3.1.7 Security Terms and Definitions

10.23.3.1.8 Related Resources

10.23.3.2 Personnel Security Responsibilities

10.23.3.3 Quality Assessment Standards

10.23.3.3.1 Investigative Service Provider (ISP) Quality Control Programs

10.23.3.3.2 Customer Agency Quality Assessment

10.23.3.4 Requirements for an Investigation

10.23.3.4.1 Transfer of Trust

10.23.3.4.2 Upgrade of Trust

10.23.3.4.3 Reestablishment of Trust

10.23.3.5 Adjudication of Background Investigations Conducted on Employees of Personnel Security and Human Capital Office Executive Team Members

10.23.3.6 Criteria for Making Suitability Determinations

10.23.3.7 Personnel Security Files

10.23.3.8 Transfer of Personnel Security Records and Clearances between Treasury Bureaus

10.23.3.9 Safeguarding and Handling Investigative Reports



10.23.3.1  
(08-05-2025)  
**Program Scope and Objectives**

- (1) **Purpose:** This revised IRM provides policy and guidance for the administration of the IRS PS operations program. Every position within the IRS requires potential employees or incumbent employees undergo a background investigation (BI) conducted by an appropriate government authority based upon the sensitivity of the position, the need for access to classified information, and the requirements of *Homeland Security Presidential Directive 12 (HSPD-12)*.
- (2) The investigative requirements must be consistent with the guidance provided by the Office of Personnel Management (OPM). Any BI, conducted for suitability or security determination purposes constitutes the first step in the process of ensuring the highest standards of honesty, integrity, and security among IRS employees. Suitability reflects the standards required for employment with the government in general, and the IRS in particular, with reference to a person's character, reputation, and overall fitness.
- (3) **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 this IRM. Should any of these instructions conflict with a provision of a negotiated agreement, the agreement prevails.
- (4) **Policy Owner:** Human Capital Office, Policy Office
- (5) **Program Owner:** Human Capital Office (HCO)
- (6) **Primary Stakeholder:** HCO, Office of Human Resource Operations (OHRO), Talent Acquisition (TA), PS, Strategic Recruitment and Hiring Services, and Hiring Operations (HOps).
- (7) **Contact Information:** *Personnel Security*

10.23.3.1.1  
(08-05-2025)  
**Background**

- (1) In March 2018, the Office of the Director of National Intelligence (ODNI) and OPM launched the "Trusted Workforce 2.0" (TW 2.0) effort, with partner agencies across the U.S. Government to fundamentally overhaul the federal personnel vetting process. The effort was designed to reduce and eliminate the background investigation backlog and establish a new governmentwide approach to personnel vetting.
- (2) The TW 2.0 policy has been finalized, and establishes new guidance for initial vetting, upgrades of trust, transfer of trust, and the reestablishment of trust as defined in Treasury Directive Publication (TD P) 15-71.

10.23.3.1.2  
(08-05-2025)  
**Authorities**

- (1) This IRM supplements policies and requirements and must be read in conjunction with cited authorities.
- (2) **Statutes:** *United State Code*
  - a. *Privacy Act of 1974, as amended, 5 USC 552a*
  - b. *5 USC 552a, Records maintained on individuals*
  - c. *5 USC 11001, Enhanced Personnel Security Programs*
- (3) **Regulations:** *Code of Federal Regulations (CFR)*
  - a. *5 CFR 1400.201, Sensitivity level designations and investigative requirements*
  - b. *5 CFR 731, Suitability*

- c. *5 CFR 732, National Security Positions*
- d. *5 CFR 736, Personnel Investigations*
- e. *32 CFR 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*
- f. *32 CFR Chapter XX, Information Security Oversight Office, National Archives and Records Administrations*

(4) **Federal Register:** *Federal Register (FR)*

- a. *60 FR 40245, Access to Classified Information*
- b. *80 FR 32243, Designation of National Security Positions in the Competitive Service and Related Matters*
- c. *Executive Order (EO) 13526, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*
- d. *EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*
- e. *EO 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*
- f. *EO 13764, Amending the Civil Service Rules, EO 13488 and EO 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*

10.23.3.1.3  
(08-05-2025)

**Roles and Responsibilities**

- (1) The Associate Director, PS, has the responsibility for adjudication of background investigations for IRS applicants/employees.

10.23.3.1.4  
(08-05-2025)

**Program Management and Review**

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

10.23.3.1.5  
(08-05-2025)

**Program Controls**

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

10.23.3.1.6  
(08-05-2025)

**Commonly Used Acronyms**

- (1) Below are commonly used personnel security acronyms.

Acronyms	Definitions
ABIS	Automated Background Investigation System
EO	Executive Order
FBI	Federal Bureau of Investigation
OPM	Office of Personnel Management
OSP	Office of Security Programs
PII	Personally Identifiable Information

Acronyms	Definitions
POC	Point of Contact
PS	Personnel Security
SBU	Sensitive But Unclassified
SF	Standard Form
TD P	Treasury Directive Publication
TSM	Treasury Security Manual

10.23.3.1.7  
(08-05-2025)  
**Security Terms and  
Definitions**

(1) Below are terms and definitions associated with this IRM:

Terms	Definitions
Access	Authority that allows an individual to obtain knowledge of, or access to, classified information, materials, or work areas.
Adjudication	An examination of a person's character or conduct over time, resulting in a favorable or unfavorable determination of their employment suitability, eligibility for access to classified information, materials, or areas, or for their retention in federal employment.
Adjudicator	A trained personnel security specialist who evaluates background investigations and other pertinent information to make employment suitability and national security eligibility determinations.
Applicant	A person who is being considered or has been considered for employment.

Terms	Definitions
Background Investigation (BI)	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.
Classified Information	Information requiring protection against unauthorized disclosure (marked CONFIDENTIAL, SECRET, or TOP SECRET when in documentary form, to indicate its classified status), pursuant to EOs 12958 and 12968.
High Risk Position	A final position designation assessment reflecting the potential for exceptionally serious impact, critical to an agency program or mission or the integrity or efficiency of the service.
Low Risk Position	A final position designation assessment reflecting the potential for limited impact on an agency program or mission or the integrity or efficiency of the service.
Moderate Risk Position	A final position designation assessment reflecting the potential for moderate to serious impact on an agency program or mission or the integrity or efficiency of the service.



Terms	Definitions
National Security Position	A position that involves activities of the government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States, and/or requires regular use of, or access to, classified information.
Office of Personnel Management	OPM is an independent federal agency that works in numerous broad areas to recruit and retain a first-rate federal workforce. One function is to provide investigative services for federal agencies to use as the basis for employee suitability, contractor fitness, and security clearance eligibility across the federal government.
Personally Identifiable Information (PII)	Also considered Sensitive but Unclassified (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 nonsensitive positions.
Public Trust Position	The category of positions, at the moderate or high-risk levels involving a significant degree of public trust (such as policy making or major program responsibilities, fiduciary responsibility, law enforcement positions, public safety, and health duties).

<b>Terms</b>	<b>Definitions</b>
Reciprocity	Recognition and acceptance of prior favorable fitness determination 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 level, investigation completed within last five years, and no break in service since the last favorable determination).
Security Clearance	Certification issued by a designated personnel security official or designee that grants an individual access to classified information, 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 from which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security, whether the occupant has access to classified information.
Suitability Action	An action described in 5 CFR 731.203 (cancellation of eligibility, removal, cancellation of reinstatement eligibility, debarment) that may be taken by OPM or an agency with delegated authority under the procedures in 5 CFR 731 subparts C and D.

Terms	Definitions
U.S. Citizen	A person born in the U.S. or its territories or born in a foreign country to U.S. born parents are U.S. citizens by birth. A person not born in the U.S. can voluntarily become a naturalized U.S. citizen once all eligibility requirements are met. Also, a minor can derive U.S. citizenship following the naturalization of one or both parents.

10.23.3.1.8  
(08-05-2025)  
**Related Resources**

- (1) *Treasury Directive 15-71*
- (2) *Treasury Order 102-01*
- (3) *Treasury Order 102-17*
- (4) *IRM 10.5.4, Privacy and Information Protection, Incident Management Program*
- (5) *IRM 10.5.8, Privacy and Information Protection, Sensitive But Unclassified Data Policy*
- (6) *IRM 10.9.1, Classified National Security Information*

10.23.3.2  
(08-05-2025)  
**Personnel Security Responsibilities**

- (1) For appointees with less than one current continuous year of service, the associate director, PS, has delegated authority to make suitability determinations and propose suitability actions under **5 CFR 731**, except for those cases that must be referred to the OPM. (Refer to **5 CFR 731.103 (f)**) The director for the Office of Human Resources Operations, Talent Acquisition, will take suitability actions under 5 CFR 731, except for those cases that must be referred to the OPM.

10.23.3.3  
(08-05-2025)  
**Quality Assessment Standards**

- (1) In January 2015, the security and suitability executive agents approved the Quality Assessment Standards (QAS) for background investigations which were distributed to federal agencies to be implemented in 2017. The QAS establishes federal guidelines for assessing the quality of national security and suitability background investigations based on the Federal Investigative Standards (FIS), implemented in December 2012. The establishment of QAS facilitates the measurement and continued improvement of investigative quality across the executive branch.
- (2) The QAS are established for background investigations to determine eligibility for:
  - a. Logical and physical access.
  - b. Suitability for government employment.
  - c. Eligibility for access to classified information and to hold a sensitive position.
  - d. Fitness to perform work for/or on behalf of the government as a contract employee.

- (3) The QAS also applies to the background investigations of state, local, tribal, and private sector entities as defined in EO 13549.
- (4) The QAS will establish how investigative quality will be defined, measured, and assessed. The QAS are not designed to determine if or what adjudicative action will be taken but to support the standardization of background investigations which, in turn, supports uniformity and reciprocity.
- (5) The QAS are based on four category assessments that characterizes the investigation as:
  1. Complete: All coverage is obtained, and all issues are resolved.
  2. Justified: Component requirement is missing but an adequate explanation is present.
  3. Incomplete: Component requirement is missing and no adequate explanation.
  4. Insufficient: Known issues not resolved and/or excessively poor reporting present.

**Note:** An investigation can be both incomplete and insufficient.
- (6) When the quality of an investigation is evaluated, it will be assigned one of the four assessment categories outlined above. The only exceptions are the investigations that are assessed as both incomplete and insufficient.

10.23.3.3.1  
(08-05-2025)  
**Investigative Service  
Provider (ISP) Quality  
Control Programs**

- (1) To ensure mechanisms are in place to identify, correct and prevent quality issues during the investigation process, every ISP that conducts investigations under the FIS will have an internal Quality Control Program.

10.23.3.3.2  
(08-05-2025)  
**Customer Agency  
Quality Assessment**

- (1) The IRS utilizes a quality assessment tool to document the quality of investigations, ensuring the assessment of the investigative quality is consistent with federal guidelines for the QAS.

10.23.3.4  
(08-05-2025)  
**Requirements for an  
Investigation**

- (1) All IRS employees are required to have an initial BI consistent with the position risk and sensitivity level identified by the Position Designation System. The PS office will initiate a BI if the following situations apply:
  - The individual is a new employee to the federal government and has never been investigated.
  - The individual is a current IRS employee and has been assigned new duties or has transferred to a new position with a higher position risk and sensitivity designation.
  - The individual had a break in service in federal employment for five years or more.
- (2) To determine if an individual meets the above situations, PS must:
  - a. Conduct searches of the governmentwide personnel vetting repositories to determine if the individual has an existing BI and/or favorable adjudication that meets or exceeds the level of investigation required for the new position.

- b. Determine if the individual is transferring from another federal agency with no break in service and has an existing BI and/or favorable adjudication. The individual will then be processed using the transfer of trust process.
- c. Determine if the individual is a current IRS employee moving to a new position or assigned new duties within the IRS and has an existing BI and/or favorable adjudication at a lower security level than the new position requires. The individual will then be processed using the upgrade of trust process.
- d. Determine if the individual had a break in service from federal employment and the duration of the break in service.
  - If the break in service is less than five years, the individual will be processed using the reestablishment of trust process.
  - If the break in service is more than five years, the individual will require a new BI.

10.23.3.4.1  
(08-05-2025)  
**Transfer of Trust**

- (1) A transfer of trust occurs when a trusted individual moves between positions. Examples would include the following:
  - a. A federal employee moves to a new agency.
  - b. A federal employee becomes a contractor.
  - c. A contractor moves from one contractor company to another.
  - d. The individual is sponsored by a different agency.
  - e. A contractor becomes a federal employee.
- (2) When receiving a transfer of trust case for adjudication, PS must determine if any of the following exist:
  - a. Reciprocity, which will apply if an investigation was completed within the past five years.
  - b. New trust determination without additional investigation.
  - Review the individual's records for the following:
    - 1. If a trust determination is missing.
    - 2. If an exception code exists.
    - 3. If the new position requires a core duty determination, then PS will make a new determination based solely upon the existing information.
- (3) New Trust Determination with Additional Vetting and/or Investigative Activity.
  - a. If the investigation exceeds the five-year deadline and the individual is not enrolled in continuous vetting (CV), or there are investigative gaps, or un-adjudicated open CV alerts that meet trigger requirements, then PS must request new standard forms from the individual and contact the ISP for additional investigative processing.
- (4) Upgrade and new trust determination required.
  - a. If a current employee is selected for a new position or duties and requires a higher tier investigation, PS will request the appropriate

standard forms and contact the ISP to conduct an upgrade investigation consistent with the new position or duties.

10.23.3.4.2  
(08-05-2025)  
**Upgrade of Trust**

- (1) An upgrade of trust occurs when an IRS employee moves into a new position or is assigned new duties within the IRS and the new position designation, or duties require an investigation at a higher security level. If PS receives a request for an upgrade of trust, PS must:
  - a. Obtain the appropriate security forms from the employee.
  - b. Request an upgrade investigation from the ISP for the new position or duties.
  - c. Ensure the employee is enrolled in the CV process consistent with the requirements of the new position or duties once a favorable adjudication is complete.

10.23.3.4.3  
(08-05-2025)  
**Reestablishment of Trust**

- (1) A reestablishment of trust occurs when an individual returns to work for or on behalf of the federal government after a break in service for less than five years.
  - a. Break in service under 36 months:
    - PS must collect new standard forms from the individual.
    - PS may contact the ISP to conduct additional investigation based on the risk assessment.
  - b. Break in service between 36 months and five years:
    - PS must collect new standard forms from the individual.
    - PS must contact the ISP to conduct additional investigation processes for the duration of the break in service.

**Note:** Exceptions to the investigative requirements may apply to certain positions that may not require an extensive BI, a suitability or fitness determination, or eligibility for access to classified national security information. Refer to Treasury Security Manual, TD P 15-71 for additional guidance.

10.23.3.5  
(08-05-2025)  
**Adjudication of Background Investigations Conducted on Employees of Personnel Security and Human Capital Office Executive Team Members**

- (1) To ensure independence of the adjudication and referral process, and to eliminate any appearance of a conflict of interest in the handling of investigative reports conducted on employees of PS and the HCO executives to whom PS directly reports, the following procedures must be effected:
  - a. All such completed reports of investigation conducted for suitability or security purposes will be made available either electronically or in hard copy to the Office of Security Programs (OSP), Department of the Treasury.
  - b. Treasury OSP adjudicates the case for suitability and clearance eligibility, as implemented in the common adjudicative standards set forth by the 5 CFR 731 and 5 CFR 732.
  - c. Treasury OSP sends an email notification regarding the completion of the investigation to Associate Director, PS.
  - d. Upon notification from Treasury, PS updates the Automated Background Investigation System (ABIS) and the Personnel Investigations Processing

System (PIPS)/Clearance Verification System (CVS) with security clearance and investigative information.

- e. PS briefs IRS employees and HCO executive team members whose cases are favorably adjudicated for access to classified information. PS provides Treasury OSP a copy of the signed Standard Form (SF)-312, Classified Information Nondisclosure Agreement for recordation purposes.
- f. PS advises Treasury OSP of any change in status of PS employees or contractors.
- g. The final determination/adjudication will be referred to Labor Employee Relations and Negotiations (LERN) only when appropriate action is recommended. Treasury OSP will maintain a copy of the report of investigation.

10.23.3.6  
(08-05-2025)  
**Criteria for Making Suitability Determinations**

- (1) PS will make post-investigation suitability determinations on employees with less than one current continuous year of service, using the specific factors contained in **5 CFR 731.202(b)**. The PS adjudicators, trained under OPM suitability guidelines, will make determinations based on a person's character and/or conduct that may have an impact on the integrity or efficiency of the IRS.

10.23.3.7  
(08-05-2025)  
**Personnel Security Files**

- (1) Per the Treasury Security Manual, TD P 15-71, Chapter 2, Section K, "Security and Suitability Operations," the IRS will establish and maintain a personnel security file for employees in the following positions:
  - a. National security positions,
  - b. Moderate and high-risk public trust positions, and
  - c. Low-risk/non-sensitive positions where unfavorable or derogatory information has been developed or received, unless the file is maintained by the OPM.
- (2) All contractors are subject to the same requirements as Treasury/IRS employees with a file maintained for contractor personnel covered by the provisions of Chapter 5, Contractor Security, of TD P 15-71 or who require a background investigation to meet the requirements of HSPD-12.
- (3) The IRS will not maintain a file on a contract employee granted access to classified information under the National Industrial Security Program (NISP), unless there is a requirement for additional investigation relating to access to Treasury/IRS facilities or automated information systems or access to classified information not covered under the NISP.
- (4) Regarding favorable investigations on employees or contractor personnel in low or moderate risk positions, the IRS will retain pertinent investigative data only, such as adverse derogatory information.
- (5) All PS files are under the control of the Associate Director, PS.

10.23.3.8  
(08-05-2025)  
**Transfer of Personnel Security Records and Clearances between Treasury Bureaus**

- (1) Per the TD P 15-71, Chapter 2, Section K, when an employee transfers from the Treasury agency office to a bureau or from one Treasury bureau to another, the complete personnel security file, or a copy of it must be transferred from the PS office of the losing bureau to the PS office of the gaining bureau. Exception: when the file of an IRS employee contains tax information, the tax information is not transferred outside the IRS.



10.23.3.9  
(08-05-2025)  
**Safeguarding and  
Handling Investigative  
Reports**

- (1) Personally identifiable information (PII) in background investigations, records, and operations must be carefully safeguarded to protect the interests of both the individual and the Service, pursuant to requirements of IRM 10.5.4, Privacy and Information Protection, Incident Management Program, and the Privacy Act of 1974. Unless classified at a higher level, personnel security information must be afforded the same degree of protection as material identified as "Controlled Unclassified Information" and must be used only for authorized official purposes. When not in use, personnel security information must be stored in a General Services Administration approved security container or in an equally secure area. All electronic records must be safeguarded in accordance with IRM 10.5.8, Privacy and Information Protection.
- (2) Reports containing classified information must be protected per EO 13526, Classified National Security Information and appropriate Treasury regulations.
- (3) The PS 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, as appropriate. Requests for the release of the results of any PS investigation should be referred to the Treasury 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 USC 552a), for the purpose of suitability or for the granting of a security clearance, the request must be made in writing to IRS, Personnel Security, PA Section, 5000 Ellin Road, Room C1-530, Lanham, MD 20706 or by fax to 855-696-0378.