EFFECTIVE DATE

(04-22-2022)

PURPOSE

(1) This transmits the revised IRM 10.23.2, Personnel Security, Contractor Investigations.

MATERIAL CHANGES

(1) IRM 10.23.2.2.1 - Changed Facilities Management and Security Services, Contractor Security Management (FMSS/CSM) to Personnel Security (PS), Contract Security On-boarding (CSO) because the responsibility for on-boarding contractor employees was transferred to PS. Clarified Contracting Officer's Representative (COR) or Business Unit (BU) official is responsible for collecting all required forms from the vendor for submission to PS/CSO.

(2) IRM 10.23.2.2.2 - Updated Selective Service registration guidance based on amended Selective Service System directives.

(3) IRM 10.23.2.2.3 - Changed the Office of Personnel Management (OPM), National Background Investigation Bureau to Department of Defense (DOD), Defense Counterintelligence Security Agency (DCSA) because the authority to conduct background investigations was transferred to DOD per Executive Order (EO)13869.

(4) IRM 10.23.2.2.4 - Updated qualified escort responsibilities to ensure escorted contractor employees do not access any areas, information, or IT systems they are not authorized to access and are properly signed out at the end of the visit.

(5) IRM 10.23.2.6 - Changed DOD system of record for suitability, eligibility, and credential management from Joint Personnel Adjudications System (JPAS) to Defense Information System for Security (DISS). JPAS was decommissioned and data transferred to DISS.

(6) IRM 10.23.2.8 - Removed outdated staff-like access definition, the revised definition is located at IRM 10.23.2.1. Clarified Security Awareness Training (SAT) must be completed before granting access to IRS-owned or controlled facilities, information technology (IT) systems, or Sensitive But Unclassified (SBU) information, etc.

(7) IRM 10.23.2.10 - Clarified SAT must be completed upon on-boarding and yearly thereafter. Added Manager of Record (MOR) is responsible for ensuring contractor employees meet SAT requirements if a COR is not assigned to the IRS contract.

(8) IRM 10.23.2.11.3 - Changed time allotted for contractor employees to response to a revocation of staff-like access determination to seven calendar days (previously 30 days for tax compliance and 14 days for all other misconduct).

(9) IRM 10.23.2.13.2 - Updated qualified escort responsibilities to ensure escorted contractor employees do not access any areas, information, or IT systems they are not authorized to access and are properly signed out at the end of the visit. Updated the authority to waive escort ratio requirements, approval by Associate Director, PS in coordination with the Associate Director, Security Policy, FMSS.

(10) IRM 10.23.2.14 - Removed two-year break in service rule based on EO 13764, which states, prior favorable fitness or suitability determinations shall be granted reciprocal recognition, to the extent practicable.

(11) IRM 10.23.2.15 - Clarified submission of documentation to initiate a reinvestigation is five years from completion of the last background investigation and not the date of the staff-like access approval memo.

(12) IRM 10.23.2.16 - Added guidance about the COR or MOR recovering and returning ID media for separating contractor employees, per IRM 10.2.5.9.

(13) IRM 10.23.2.22 - Updated background investigations are funded by the Human Capital Office (previously funded by the requesting customer's organization).

(14) IRM 10.23.2.23 - Updated acceptance of previously completed investigation to within last five years (previously within last two years) and removed two-year break in service rule.

(15) Throughout the IRM, updated organizational titles, updated security terms, revised language to improve readability, updated links, and made other minor editorial changes.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 10.23.2, Personnel Security, Contractor Investigations dated April 29, 2019.

AUDIENCE

All Business Units

Kevin Q. McIver
IRS Human Capital Officer

10.23.2
Contractor Investigations

Table of Contents

10.23.2.1
(04-29-2019)
Program Scope and Objectives

(1) **Purpose.** This section provides policy and describes the background investigative requirements for contractors (and contractor personnel), subcontractors (and subcontractor personnel), and those providing advisory and assistance services to determine their fitness for work on IRS contracts. Hereafter the term **IRS contract** refers to contracts, solicitations, orders, and awards for services (e.g., courier, mail, or janitorial services, etc.) granted by an IRS official, under which contractor (including subcontractor) employees require staff-like access to IRS-owned or controlled facilities (includes leased or contracted space), IT systems, SBU information, or security items or products. These individuals (all of whom are collectively referred to hereinafter, as "contractor employees," as appropriate) include but are not limited to:

- Outside Experts
- Consultants
- Courier and Printing Services
- Sign Language Interpreters
- Document Recovery Services
- Delivery Services
- Interns (paid/unpaid)

Special emphasis and discussion are placed on those contractors who require staff-like access, wherever the location, to IRS-owned or controlled facilities; or work on contracts (as defined in *Federal Acquisition Regulation (FAR) Part 2* that involve the design, operation, repair, or maintenance of IT systems; and/or require access to SBU information as defined in IRM 10.5.1.2.2, Sensitive But Unclassified Information.

Staff-like Access is authority granted to perform one or more of the following:

a. Enter IRS facilities or space (owned or leased) unescorted (when properly badged);
b. Possess login credentials to information systems (IRS or vendor-owned systems that store, collect, and /or process IRS information);
c. Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) SBU information, wherever the location; (Refer to IRM 10.5.1 for examples of SBU information);
d. Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room, wherever the location. These items include, but are not limited to security devices/records, computer equipment, identification media. For details and further security requirements, refer to IRM 10.2.15, Minimum Protection Standards); or
e. Enter physical areas, wherever the location, that store/process SBU information (unescorted).

Note: The above standard does not define policy for storing or protecting classified National Security Information (NSI). For guidance, refer to IRM 10.9.1, Classified National Security Information.

Staff-like Access is granted to an individual who is not an IRS employee (and includes but is not limited to the contractor employees described above) and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.

This manual does not prescribe policy with respect to issuance of security clearances for access to classified NSI under the Defense Counterintelligence Security Agency (DCSA), *National Industrial Security Program* (NISP). For guidance about contract requirements for contractor's access to NSI, refer to IRM 10.9.1.10, Contractors and NSI.

(2) **Audience.** The policy and guidance in this IRM apply to all business units.

(3) **Policy Owner.** IRS Human Capital Officer.

(4) **Program Owner.** Human Capital Office Policy and Audits and Personnel Security, Talent and Acquisition (TA) Division.

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

10.23.2.1.1
(04-22-2022)
Authority

(1) Contractor employees with staff-like access must comply with the provisions of:

a. *EO 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters, 17 Jan 2017.*
b. *EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, 16 Jan 2009 (as amended).*
c. *EO 13467, Reforming Processing Related to Suitability for Government Employee, Fitness for Contractor Employees, and Eligibility to Access National Security Information, 2 Jul 2008 (as amended).*
d. *EO 13869, Transferring Responsibility for Background Investigations to the Department of Defense, 24 Apr 2019.*
e. *Title 5, Code of Federal Regulations (CFR), Part 731, Suitability.*
f. *Title 5 CFR, Part 736, Personnel Investigations.*
g. *Treasury Directive Publication (TD P) 15-71, Chapter II, Section 2, Investigative Requirements for Federal Employees, Contractors, Subcontractors, Experts, Consultants and Paid/Unpaid Interns.*
h. *Treasury Order 102-17, Delegation of Authority Concerning the Personnel Security.*
i. *IRS Delegation Order 10-1, Perform Operating Functions Relating to Personnel Security.*
j. IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance.
k. *IRS Publication 4812, Contractor Security & Privacy Controls.*

10.23.2.1.2
(04-29-2019)
Roles and Responsibilities

(1) PS is responsible for the adjudication of background investigations for contractor employees. PS adjudicators, trained under OPM suitability guidelines, makes a fitness determination based on the individual's character and/or conduct to work for the IRS as a contractor employee.

10.23.2.1.3
(04-22-2022)
Program Management and Review

(1) PS will collaborate with Procurement and FMSS related to non-IRS employees/contractors who need staff-like access on an as-needed basis but no less than once every three years to evaluate the program effectiveness and implement changes, as warranted.

10.23.2.1.4
(04-29-2019)
Commonly Used Acronyms

(1) The table lists commonly used acronyms.

Acronym	Definition
ABIS	Automated Background Investigation System
COR	Contracting Officer's Representative
CSO	Contractor Security On-boarding
DCSA	Defense Counterintelligence and Security Agency
EO	Executive Order
FBI	Federal Bureau of Investigation
LPR	Lawful Permanent Resident
MOR	Manager of Record
NDA	Non-Disclosure Agreement
NISP	National Industrial Security Program
NSI	National Security Information
OPM	Office of Personnel Management
OSP	Office of Security Programs (Treasury)
PDT	Position Designation Tool
POC	Point of Contact
PS	Personnel Security
RAC	Risk Assessment Checklist
SAT	Security Awareness Training
SBU	Sensitive But Unclassified
TD P	Treasury Directive Publication
TSM	Treasury Security Manual

10.23.2.1.5
(04-29-2019)
Security Terms and Definitions

(1) For Security Terms and Definitions, refer to IRM 10.23.2.23.

10.23.2.2
(04-27-2016)
General Investigative Requirements

(1) Unless specified otherwise in this IRM, each contractor employee assigned to work under an IRS contract shall undergo investigative processing commensurate with the position risk level designation associated with the work to be performed, and comparable to that required for federal employees who occupy the same positions and who have the same position risk designation.

(2) Investigative requirements also apply when permitting contractor employees staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products even if no formal contract was awarded by Procurement. In such instances, the responsibility for meeting investigative requirements described in this IRM rests with the BU authorizing access for these contractor employees.

10.23.2.2.1
(04-22-2022)
Vendor and Contracting Officer's Representative Roles

(1) The vendor (company under contract) will assign a Point of Contact (POC) to all IRS contracts requiring staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products.

(2) The vendor POC will assist the COR or the appropriate BU official (individual who procured the contract) regarding position duties, level of staff-like access required, preliminary assessments of the position risk designation, and the collection of required forms/documentation.

(3) PS/CSO sends the Master Survey/Position Designation Survey and other forms to the vendor POC and the COR.

(4) The COR or the appropriate BU official (individual who procured the contract) and the vendor POC will review the work to be performed under contract to assign a position risk designation. A risk assessment must be conducted for each position on the contract in accordance with the criteria in TD P 15-71, Chapter I, Section 1, Position Sensitivity and Risk Designation and IRM 10.23.2.5, Position Risk Designations.

(5) The COR or the appropriate BU official will collect the Master Survey/Position Designation Survey and all required forms from the vendor POC and review for completeness and accuracy before submitting to PS/CSO for processing.

(6) PS/CSO will coordinate the background investigation submissions and actions with the COR, as appropriate.

Note: **A background investigation should not be initiated until a contract number is assigned to the vendor who is awarded the contract and the contractor employee is assigned to perform work on the IRS contract.**

10.23.2.2.2
(04-22-2022)
Eligibility Criteria

(1) Contractor employees hired for work within the United States or its territories and possessions who require staff-like access, wherever the location, to IRS-owned or controlled facilities, SBU information, security items or products; or work on contracts that involve the design, operation, repair, or maintenance of IT systems, must meet the eligibility criteria listed below before being considered for staff-like access and initiating a background investigation.

(2) The above does not apply to non-federal personnel who do not have a contract with the IRS (i.e., childcare workers, Credit Union employees) as they have access to non-IRS and public IRS areas only. Such personnel are vetted through their respective agency.

Note: Eligibility criteria apply to escorted contractor employees **only** when the contractor employee requires staff-like access and the interim staff-like access determination is pending. During this period, the contractor employee is allowed temporary escorted access to IRS facilities **only**, with **no** access to IT systems, SBU information, security items or products. Escorted access should only be used in emergency situations (e.g., when a contractor employee needs to attend a kickoff or other meeting scheduled prior to interim staff-like access being granted).

a. Must be federal tax compliant. Must have filed all required tax returns and paid all taxes due or be current on a payment plan for taxes due. Contractor employees **must** remain tax compliant while actively working on IRS contracts.

   Note: Periodic tax checks will be conducted on all IRS contractor employees who have been granted staff-like access by PS and remain active on an IRS contract, refer to IRM 1.2.1.16.2, Policy Statement 25-3, Standard Tax Compliance Checks for Suitability and Monitoring for Federal Applicants, Employees, and Contractors. This is in addition to the tax check conducted at the initial on-boarding of contractor employees requiring staff-like access and contractor employees undergoing revalidation of staff-like access. All tax checks are conducted using the Tax Check Application, Tax Check Compliance Service. PS is responsible for requesting the tax check through the Privacy, Governmental Liaison & Disclosure Office.

b. Must meet the following U.S. citizenship or residency requirements based on the assigned position risk level.

Position Risk Level	**Citizenship or Residency Requirement**
Low Risk	U.S. citizen or Lawful Permanent Resident (LPR)
Moderate Risk	U.S. citizen or LPR with at least three consecutive years of U.S. residency from the date of legal entry as an LPR.
High Risk	U.S. citizen

c. All males born after 1959 must be registered with Selective Service. If not registered or exempt, the contractor must have a Status Information Letter from Selective Service. For information about who needs to register, visit *https://www.sss.gov/register/who-needs-to-register/*
   1. Immigrant males between ages 18 and 25 are required by law to register with the Selective Service within 30 days of arriving to the U.S. This includes naturalized citizens, parolees, undocumented immigrants, LPR, asylum seekers, refugees, and all males with visas more than 30 days expired.
   2. If an immigrant male did not register and is between the age of 26 and 31, a Status Information Letter is required.
   3. Non-Immigrant males living in the U.S. on a valid visa are not required to register if they remain on a valid visa up until they turn 26. However,

he must provide a copy of official documentation of his first entry into the U.S. For a list of acceptable documents, visit*https://www.sss.gov/wp-content/uploads/2020/02/DocumentationList.pdf*

(3) Vendors must ensure that foreign born contractor employees meet the eligibility requirement for U.S. citizenship or LPR status and when applicable, Selective Service requirements. The Selective Service Online Registration Verification website at *https://www.sss.gov/Home/Verification* is available for a status check.

(4) Investigative processing is required regardless of the location of the work. This includes contractor employees who use technology for remote staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products.

10.23.2.2.3
(04-22-2022)
Background Investigation

(1) All contractor employees who work on IRS contracts that require staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products must be investigated. The investigation must be favorably adjudicated. The investigation covers various components of an individual's personal background, and a credit check is a standard part of many of these investigations. Contractor employees are required to sign a release form authorizing a search of their credit history. Refer to IRM 10.23.3.3, Credit Checks.

(2) IRS contractor employees who require background investigations as follows:

a. Contractor employees whose duration of employment exceeds 180 calendar days per year are subject to the following prior to beginning work on the IRS contract. Example: If a contractor employee works every other month which exceeds 180 days during the calendar year, the criteria will apply.
1. Must meet the eligibility requirements for staff-like access outlined in IRM 10.23.2.2.2.
2. Must receive a favorable interim staff-like access determination from PS based on a review of a Federal Bureau of Investigation (FBI) fingerprint check and a review of investigative paperwork completed by the contractor employee.
3. A background investigation must be initiated by PS and scheduled by the DCSA based on the assigned position risk designation.

Note: The completed background investigation must be adjudicated to determine if the contractor employee can continue to perform work on the contract. If a prior investigation meets reciprocity criteria, a new investigation is not required.

b. If the duration of employment is less than 180 calendar days per year and the contractor employee requires staff-like access to IRS-owned or controlled facilities, IT systems, SBU information or security items or products, the contractor employee is subject to the following prior to beginning work on the IRS contract:
1. Must meet the eligibility requirements for access in IRM 10.23.2.2.2.
2. Must have an approved staff-like access determination (meet the eligibility requirements and have a favorably adjudicated FBI fingerprint check).

c. There are re-investigation requirements for contractor employees in low, moderate, and high risk positions, refer to IRM 10.23.2.15. Additionally,

contractor employees are subject to investigation at any time during the period of access to determine whether they continue to meet the requirements for staff-like access.

10.23.2.2.4
(04-22-2022)
Infrequent Access to Facilities and Equipment

(1) For contractor employees who do not require staff-like access to IRS IT systems or SBU information and only require infrequent access to IRS-owned or controlled facilities and/or equipment (e.g., a time and material maintenance contract that warrants access one or two days monthly/quarterly) as described in 10.23.2.13; no background investigation is required if the contractor employee receives 100% escort by a qualified escort. Refer to IRM 10.2.5.6.3, Non-Photo ID Cards and IRM 10.2.18.5, Physical Access Eligibility Requirements.

(2) A **qualified escort** is an IRS employee, or a contractor employee approved for staff-like access at the same or higher position risk level as the escorted contractor employee. At least one **qualified escort** can escort up to five escorted persons. Refer to IRM 10.2.18.5.2, Escorted Access. The qualified escort must:

a. Accompany the contractor employee during all work performance and movements throughout the facility.
b. Maintain visual contact with the escorted contractor employee.
c. Ensure escorted contractor employee does not access any areas, information, or IT systems they are not authorized to access.
d. Accompany the escorted contractor employee to sign out and return any ID media at the end of the visit.

10.23.2.2.5
(04-29-2019)
Access to Facilities in a Foreign Country

(1) Contractor employees requiring access to IRS-owned or controlled facilities or space in foreign countries who have been certified by the Department of State Diplomatic Security Service as meeting investigative and adjudicative criteria for access to facilities, under the authority of a Chief of Mission, will be deemed to meet personnel security standards. In these cases, a review and determination by PS is still required to ensure IRS specific standards are met.

10.23.2.2.6
(04-29-2019)
Retention of Personnel Security Files

(1) IRS will establish and maintain a personnel security file for each contractor employee in the following conditions:

a. All moderate and high risk positions; and
b. Those low risk or non-sensitive positions on which unfavorable or derogatory information has been developed or received unless the file is maintained by OPM.

(2) IRS will not maintain a file on a contractor employee granted staff-like access to classified NSI under the NISP, unless there is a requirement for:

a. Additional investigation in connection with access to IRS facilities or automated information systems; or
b. Access to classified NSI not covered under the NISP.

(3) For favorable investigations on contractor employees in low or moderate risk positions, IRS may, at their discretion, retain either the entire report or pertinent investigative data only. The specific location of personnel security

files shall be at IRS discretion with the following exception: all national security files shall be maintained by the Treasury Personnel Security Officer or Associate Director, PS.

(4) Personnel security files must be maintained and destroyed in compliance with Document 12990, IRS Records Control Schedule, Document 12 Personnel Security Records, Item 2.

10.23.2.3
(04-29-2019)
Citizenship Requirements

(1) In accordance with TD P 15-71, contractor employees hired for work within the United States or its territories and possessions and who require staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products, shall either be U.S. citizens or have LPR status.

(2) IRS will adhere to the following standard when allowing contractor employees staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products:

Position Risk Level	Citizenship or Residency Requirement
Low Risk	U.S. citizen or LPR
Moderate Risk	U.S. citizen or LPR with at least three consecutive years of U.S. residency from the date of legal entry as an LPR.
High Risk	U.S. citizen

10.23.2.3.1
(04-29-2019)
Citizenship Waiver Requirements

(1) Only under exceptional circumstances should a waiver be requested when a contractor employee does not meet the U.S. citizenship or LPR residency requirement.

(2) Foreign nationals employed as contractor employees shall not be allowed staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products before the issuance of a waiver. For contractor employees not meeting conditions in IRM 10.23.2.2.2, a waiver may be requested as follows.

a. Low risk: Waiver may be requested by the COR.
b. Moderate risk: Waiver may be requested by the COR through a senior executive-level manager in the business unit that holds the contract.
c. High risk: Waiver request will **not** be considered for foreign nationals.

(3) Waivers for foreign nationals working in IT positions involving the development of IRS hardware or software products will **not** be considered if the position involves:

a. The design of security models, application integration, customization of software or hardware, or configuration of servers or networks; and/or
b. The ability to manipulate, alter or affect the integrity, accessibility or availability of IT-maintained information or records.

10.23.2.3.2
(04-29-2019)
Submitting a Waiver Request

(1) Requests for waivers to the citizenship requirement must be submitted in writing to the Associate Director, PS, who will forward it to the Director, OSP, Department of the Treasury, for a final determination. All waivers involving IT systems must be routed through Treasury's Chief Information Officer for a final determination.

(2) All waiver requests must include the following:

a. The full name, date of birth, place of birth, and current citizenship of the contractor employee.
b. A completed SF85, SF85P, or SF86.
c. A completed background investigation.
d. A description of the job/duty to be performed.
e. Justification why there is no qualifying U.S. citizen or permanent resident alien available or capable of performing the task.
f. A business case necessitating the waiver.
g. An assessment of the risk associated with granting the waiver.
h. All security countermeasures and actions taken to mitigate the risks associated with the requested waiver.

10.23.2.4
(04-29-2019)
Fingerprinting Contractor Employees

(1) PS/CSO is responsible for sponsoring contractors in USAccess. The contractor employee will:

a. Schedule required appointment at USAccess enrollment station via e-mail notification sent to the contractor employee. The USAccess system is the first choice.
b. If USAccess fingerprinting is not readily available, contractor employees may use Live Scan fingerprinting services at limited local servicing IRS Offices or IRS approved enrollment stations.
c. If an enrollment station is not available, FMSS Identity Credential and Access Management may delegate escort and/or registrar responsibilities to CORs to escort contractor employees to other locations for fingerprinting.

(2) In rare instances, ink and roll fingerprints will be taken by IRS Offices or approved enrollment stations. The authorized representative should complete two fingerprint cards for each contractor employee.

(3) The integrity of the chain of custody of the completed ink and roll fingerprint card must be maintained; therefore, the completed fingerprint card must be mailed directly to PS/CSO by the entity administering the fingerprinting.

(4) When the contractor employee will not have physical or systems access, non-custodial fingerprints taken at police or law enforcement offices can be utilized. The chain of custody requirement in HSPD-12 is not required for these contractor employees.

(5) Any costs for fingerprinting outside an IRS office (except for an IRS approved enrollment station) will be borne by the contractor vendor or contractor employee.

10.23.2.5
(04-27-2016)
Position Risk Designations

(1) Every IRS position, including those of contractor employees, must be designated with a position risk designation. Contractor employees must meet personnel suitability standards commensurate with their position risk designation. Refer to IRM 10.23.3.4, Scope of Position Designation System.

10.23.2.5.1
(04-29-2019)
Determining the Position Risk Designation

(1) The vendor POC and COR or BU official (individual who procured the contract) are responsible for working with the appropriate business unit management for identifying access needs and preliminary assessments on risk designations for each position within the contract. The Associate Director, PS, has the ultimate authority for position risk designation and may adjust the risk level if deemed appropriate.

(2) These position risk levels are established through an analysis of the duties and responsibilities of the positions, the placement of contractor employees and their potential impact on the agency's mission. All position risk designations will be determined using the Master Survey/Position Designation Survey, which provides a logical questionnaire-based approach to position risk designation.

10.23.2.5.2
(04-29-2019)
Position Risk Designation for IT Privileged Access

(1) Contractor employees in IT positions with **IT Privileged Access** to sensitive IT systems must be designated as high risk.

a. IT management must identify these contractor employees and enter a request into the Business Entitlement Access Request System (BEARS).
b. PS will determine if an adequate investigation exists or if a new investigation is required for the high risk position.
c. Access will be granted if a requisite background investigation exists or upon the completion and favorable adjudication of a new background investigation for the high risk position.
d. **IT Privileged Access** is defined as administrator or root access to DS, DSTEST and IRSNET domains and that contain highly sensitive, critical information. Individuals with this level of access have major program responsibilities and authorities; and if information is compromised, it could cause exceptionally serious damage to the national financial market. Examples of DS, DSTEST and IRSNET domains include, but not limited to:

- IBM and application access Individual Master File (IMF)
- Business Master File (BMF)
- Customer Account Data Engine (CADE/CADE2)
- Redesigned Revenue Accounting System (RRACS)
- Integrated Financial System (IFS)
- Corporate Files On-Line (CFOL)

10.23.2.6
(04-22-2022)
Interim Staff-like Access Approval

(1) Interim staff-like access approval may be granted prior to the completion of the background investigation. Due to the risk associated with granting staff-like access prior to the completion of the required background investigation, interim staff-like access will only be granted in cases where it has been determined that the risk is acceptable.

(2) Contractor employees who have been approved for interim staff-like access are granted staff-like access while in IRS-owned or controlled facilities (includes leased or contracted space), except for designated limited areas. Refer to IRM 10.2.18.5.1, Unescorted Access and IRM 10.2.18.8, Limited Area Access.

Note: Contractor employees in IT positions with **IT Privileged Access** to IRS sensitive IT systems, designated as a high risk position, will **not** be granted interim staff-like access.

(3) Interim staff-like access approval is based on the following eligibility/suitability checks:

a. Background investigation forms
b. IRS account history for federal tax compliance
c. Selective service registration compliance
d. Citizenship/residency
e. FBI fingerprint criminal history
f. If applicable, credit history report
g. If applicable, prior background investigations

(4) Contractor employees who possess a current active U.S. Government security clearance for access to classified NSI may be granted interim staff-like access for positions after:

a. The security clearance is verified through the Defense Information Security System (DISS).
i. Top Secret. Interim staff-like access approval to occupy positions designated at High, Moderate or Low risk.
ii. Secret or Confidential. Interim staff-like access approval to occupy positions designated Moderate or Low risk.
b. A favorable adjudication of pre-screening eligibility/suitability checks.

10.23.2.6.1
(04-29-2019)
Notification of Interim Staff-like Access

(1) If preliminary security checks are favorable, the COR will receive a memorandum of notice of interim staff-like access approval. When the results are unfavorable, the COR will receive a notice of interim staff-like access denial.

(2) Access to IT systems and/or SBU information **cannot** granted before interim staff-like access is approved.

(3) The memorandum of notice of interim staff-like access approval shall be attached to the Request for ID Media/Access Card for Contract Employee application. For system access, the COR must have this memorandum of notice of interim staff-like access approval on file before initiating an Information System User Registration/Change Request in BEARS. The COR will inform contractor employee of ID card pick up procedures.

Note: Regardless of where work is performed, contractor employees who require a password or access to an IRS IT system must be approved for staff-like access before initiating a system access request in BEARS.

(4) Contractor employees who require staff-like access to IRS-owned or controlled facilities, IT systems SBU information, or security items or products, regardless of location, must complete mandatory SAT before access is granted as described in IRM 10.23.2.10.

10.23.2.6.2
(04-22-2022)
Proposed Denial or Revocation of Interim Staff-like Access

(1) If PS issues the contractor employee a Proposal to Deny letter during the interim staff-like access determination process, the contractor employee **cannot** enter on duty and/or perform work on the contract until a final staff-like access approval determination is rendered.

(2) If interim staff-like access is approved and then subsequently a proposal to revoke letter is issued, staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products must be immediately suspended by the COR until a final determination is made by PS.

10.23.2.7
(04-22-2022)
Reciprocity of Other Agency Background Investigations

(1) PS will accept background investigations and adjudications conducted by other federal agencies unless it is determined that the background investigation or adjudication does not sufficiently address the standards used by PS in determining contractor fitness.

(2) Completed background investigations and final favorable adjudications will be accepted for staff-like access unless:

a. The new position requires a higher level investigation;
b. Favorable adjudication or background investigation was completed more than five years ago;
c. New adverse information is obtained that questions the individual's fitness for staff-like access based on character or conduct; or
d. The individual's investigative record shows conduct that is incompatible with core duties of the new position.

(3) Additional requirements must be met for all position risk levels for final staff-like access to be granted: fingerprint screening, selective service registration, citizenship/residency requirements and full federal tax compliance.

10.23.2.8
(04-22-2022)
Final Staff-like Access

(1) Contractor employees who have been approved for final staff-like access, based on a favorably adjudicated background investigation, are granted staff-like access while in an IRS-owned or controlled facility (which includes leased or contracted space), except for designated limited areas. Refer to IRM 10.2.18.5.1, Unescorted Access and IRM 10.2.18.8, Limited Area Access.

Note: Staff-like access to work on IRS contracts does not constitute a national security clearance and does not allow access to classified NSI.

(2) Contractor employees who require staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products, regardless of location, must complete mandatory SAT before access is granted as described in IRM 10.23.2.10.

10.23.2.8.1
(04-29-2019)
Access to IT Systems and Sensitive Information

(1) Contractor employees approved for staff-like access may be granted access to IT systems or SBU information no matter where the work will be located. This access is not unlimited and should only be granted to accomplish the work described in the IRS contract. Until a contractor employee has been approved for staff-like access, an escort is required no matter where the work is located and **no** access to IT systems or SBU information is permitted. For escort procedures, refer to 10.23.2.13 below.

(2) SBU information is any 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. Refer to IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data. Examples of SBU information include:

a. Personal information, including employment information such as job applications, disciplinary actions, performance appraisals, drug tests and health exams.
b. Tax return information (IRC 6103).
c. Law enforcement manuals.
d. Certain procurement documents, bids, and contracts.

(3) Personally Identifiable Information (PII) is also considered SBU information. This is information that is linked or linkable to an individual and the information must be protected to prevent the possibility of identity theft or invasion of privacy. Examples include:

a. Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history.
b. Information that can be used to distinguish or trace an individual's identity such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc.

10.23.2.9
(04-29-2019)
Notification of Final Staff-like Access Determination

(1) When the investigation is completed and the results are favorable, PS will e-mail the COR a memorandum of notice of final staff-like access approval.

(2) The memorandum of notice of final staff-like access approval must be attached to the Request for ID Media/Access Card for Contract Employee application. For system access, the COR must have this memorandum of notice of final staff-like access approval on file before initiating a BEARS, Information System User Registration/Change Request. The COR will inform contractor employee of ID card pick up procedures.

Note: If the contractor employee was approved for and retained interim staff-like access, issued an ID card, and granted system access; the above step is not required for final staff-like access approval.

(3) When the results of the investigation are unfavorable and final staff-like access is not granted, PS will email the COR a memorandum of notice of final staff-like access denial. Refer to IRM 10.23.2.11 for more details of actions taken when the results are unfavorable.

10.23.2.10
(04-22-2022)
Security Awareness Training (SAT) Requirements

(1) Contractor employees who require staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products, regardless of location, must complete mandatory SAT upon on-boarding and yearly thereafter.

(2) The COR or Manager of Record (MOR) is responsible for ensuring contractor employees receive SAT within five business days of being granted interim/final staff-like access. This training must be completed before being granted access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products. The SAT results must be uploaded in the Integrated Talent Management system to maintain staff-like access. For more information about SAT, refer to IRM 10.8.1.3.2, AT-1 Awareness and Training Policy and Procedures and for physical access, IRM 10.2.18, Physical Access Control .

(3) If the contractor employee has **IT Privileged Access**, the COR or MOR is responsible for ensuring the contractor employee completes the Specialized IT Security Training pertinent to their roles and responsibilities before being granted access to the IT system or performing assigned duties. Contractor employees with such access are required to complete specialized training annually. Refer to IRM 10.8.1.3.2.2, AT-3 Role Based Training and IRM 10.8.2, Information Technology (IT) Security, IT Roles and Responsibilities.

10.23.2.11
(07-28-2014)
Adverse Information - Denial and Revocation of Final Staff-like Access

(1) When adverse information is discovered or detected during an investigation, the scope of the inquiry may be expanded to obtain additional information to determine whether the contractor employee may continue staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products.

(2) If adverse information that may warrant action is discovered during a background investigation, the contractor employee must be so advised and offered an opportunity to refute, explain, clarify, or mitigate the information in question. The contractor employee will be advised that the IRS will not disclose any details of the adverse information to the vendor.

(3) If after final adjudication, a determination is made of ineligibility to render services on a contract and access to IRS-owned or controlled facilities is denied, the contractor employee will be formally notified and informed of the decision and the reason(s). The vendor will be advised only that the contractor employee is denied employability on the IRS Government funded contract. This decision does not intend to imply that the contractor employee's suitability for employment elsewhere in the company is affected.

10.23.2.11.1
(04-22-2022)
Proposed Denial of Final Staff-like Access

(1) If during final adjudication, a proposal to deny letter for final staff-like access is issued, PS will:

a. Email a proposal to deny letter to the contractor employee. The letter will outline the reasons for the proposed staff-like access denial and the contractor employee will have seven calendar days, from the date of receipt, to respond to PS.
b. Notify the COR that the contractor employee is being denied staff-like access for reasonable cause until a final determination is made. The COR must ensure that the contractor employee's staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products is immediately suspended until the final determination is made.
c. Render a final determination upon receipt of the contractor employee's response or expiration of the time allotted for the contractor employee to respond. The contractor employee and COR will be notified in writing of the final decision and any required actions.

10.23.2.11.2
(04-29-2019)
Notification of Denial of Final Staff-like Access

(1) If after final adjudication, PS decides to deny final staff-like access, notification of this decision will be e-mailed to the contractor employee.

a. PS will notify the COR with a Memorandum of Notification of Final Staff-like Access Denial.
b. The COR will notify the Contracting Officer (CO) to remove the contractor employee from the contract.

(2) The CO (or COR if authorized to communicate with the vendor under this circumstance) must take the following steps:

a. Communicate to the vendor the contractor employee is being denied final staff-like access for reasonable cause. Such finding makes the contractor employee ineligible to render services (or otherwise perform) under the IRS contract, and the decision by the government does not intend to imply that the contractor employee's suitability for employment elsewhere in the company is affected.

b. Provide a copy of the Memorandum of Notification of Final Staff-like Access Denial to the vendor. PS will not disclose any details of the adverse information to the vendor, COR, or third-party entity.
c. Immediately remove the contractor employee from the IRS contract.

Note: If the contractor employee performs work on more than one IRS contract, the contractor employee must be removed from all contracts unless the reason for the denial does not have a nexus to duties being performed on the contract. This includes situations where access only occurs at an off-site or non-IRS location.

d. Retrieve all ID media, keys, and/or sensitive information from the contractor employee.
e. Disable all IT system user accounts associated with the contractor employee.

10.23.2.11.3
(04-22-2022)
Revocation of Final Staff-like Access

(1) Staff-like Access to /IRS-owned or controlled facilities, IT systems, SBU information, or security items or products is a privilege. It may be revoked by the contracting IRS element based upon unsanctioned, negligent, or willful action on the part of a contractor employee. Examples of actions that can trigger revocation include, but are not limited to:

a. Non-compliance with federal tax regulations.
b. Unauthorized access or inspection of a sensitive system and/or data.
c. Introduction of unauthorized and/or malicious software.
d. Unauthorized modification or disclosure of systems and/or data.
e. Failure to follow prescribed access control policies or procedures.

(2) When revocation of staff-like access is appropriate, PS will:

a. Email a proposal to revoke staff-like access letter to the contractor employee. The letter will outline the reasons for the proposed action and the contractor employee will have seven calendar days, from the date of receipt, to respond to PS.
b. Notify the COR that the contractor employee's staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products is being suspended for reasonable cause until a decision is made.
c. Render a final determination to revoke or grant continued staff-like access upon receipt of the contractor employee's response or expiration of the allotted time for the contractor employee to respond. At such time, the contractor employee and the COR will be notified in writing of the final decision and any required actions.

(3) If staff-like access is revoked, the CO (or COR if authorized to communicate with the vendor under this circumstance) must take the following steps:

a. Communicate to the vendor that the contractor employee's staff-like access is being revoked for reasonable cause. Such finding makes the contractor employee ineligible to render services (or otherwise perform) under the IRS contract, and that the decision by the Government does not intend to imply that the contractor employee's suitability for employment elsewhere in the company is affected.
b. Provide a copy of the Memorandum of Notification of Final Staff-like Access Revocation to the employer. PS will not disclose any details of the adverse information to the vendor, COR, or third-party entity.

c. Immediately remove the contractor employee from the IRS contract.
d. Retrieve all ID media, keys, and/or sensitive information from the contractor employee.
e. Disable all IT system user accounts associated with the contractor employee.

10.23.2.12 (04-29-2019) **Staff-like Access for Other Federal Agency Personnel**

(1) Other federal agency personnel who require periodic access, on a recurring basis, may be granted staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products. The individual must have a completed and favorably adjudicated background investigation at, or higher, than the risk level of the work to be performed or the access to the controlled IRS work area. The background investigation and adjudicative determination must be verified through the parent agency's security office and/or the appropriate OPM security indices. Refer to the following standard operating procedures, which are located on the *PS Website*.

- Clearing Other Federal Agency/Bureau Personnel (not paid for by the IRS) for Unescorted Access to IRS Facilities/Data/Systems (SOP PS 4-1A)
- Clearing Other Federal Agency/Bureau Personnel (being paid by the IRS) for Unescorted Access to IRS Facilities/Data/Systems (SOP PS 4-1B)
- Clearing Department of Homeland Security (DHS) Federal Protective Service (FPS) Security Officers for Unescorted Access to IRS Facilities/Data/Systems (SOP PS 4-1C)

10.23.2.13 (04-29-2019) **Escort Procedures**

(1) Contractor employees must be escorted in the following instances, but will **not be permitted** to access IRS IT systems or SBU information:

a. When a background investigation has been initiated and an interim staff-like access determination is pending.

Note: In the event a proposal to deny or revoke interim staff-like access letter is issued, all access will be immediately suspended until a final staff-like access determination is made. Refer to IRM 10.23.2.6.2, Proposed Denial or Revocation of Interim Staff-like Access.

b. In lieu of an investigation when the contractor employee requires infrequent access to an IRS-owned or controlled facility or equipment and no access to IRS IT systems or SBU information is required.

10.23.2.13.1 (04-29-2019) **In Lieu of Investigation**

(1) Alternative 10.23.2.13(1)b above, **in lieu of investigation,** applies **only** to contractor employees who require infrequent access to a facility or equipment (e.g., a time and material maintenance contract that warrants access one or two days monthly/quarterly). Under these special circumstances, a management official, in the requesting organization, may opt to provide escort access to a contractor employee instead of initiating a background investigation. Refer to IRM 10.2.5.6.3, Non-Photo ID Cards.

Note: This alternative **does not apply** to contractor employees who have **frequent** access to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products.

(2) Prior to selecting this alternative, the management official must adhere to the following conditions, in addition to the requirements set forth in IRM 10.23.2.13.2.

a. Ensure escort access provides adequate security protection.
b. Document the decision and provide a copy to the COR.
c. Coordinate escort with management official at the site(s) where access is required.

10.23.2.13.2
(04-22-2022)
Escort Requirements

(1) Escorted access requirements are the same for work performed at any IRS-owned or controlled facility. Requirements for escorted access are:

a. Only an IRS employee or contractor employee approved for final staff-like access at the same or higher position risk level, as the escorted contractor employee, can serve as a qualified escort.
b. At least one **qualified escort** can escort up to five escorted persons. Refer to IRM 10.2.18.5.2, Escorted Access.
c. The escorted contractor employee must be accompanied during all work performance and movement throughout the facility.
d. At a minimum, the qualified escort must maintain visual contact with the escorted contractor employee.
e. Ensure the escorted contractor employee does not access any areas, information, or IT systems they are not authorized to access.
f. At the end of the visit, accompany the escorted contractor employee to sign out and return any ID Media.

Note: Exceptions to these requirements must be approved by the Associate Director, PS, in coordination with the Associate Director, Security Policy, FMSS.

(2) Contractor employees who have been denied final staff-like access **cannot be escorted** and must be removed from the IRS contract unless the contractor employee performed on more than one contract and was not removed from all IRS contracts, refer to IRM 10.23.2.11.2 (2) c.

10.23.2.14
(04-22-2022)
Revalidation of Contractor Employee Staff-like Access

(1) When there is a material change in the IRS contract or working situation, re-validation of staff-like access is required for the affected contractor employee(s). Examples of material changes include:

a. Contractor employee transfers from one IRS contract to another.
b. Contractor employee requires access to more than one IRS contract.
c. Contractor employee separates from an IRS contract.
d. Contractor employee name change.
e. Contractor company name change.
f. Contract number change.

(2) In these situations, the following will occur:

a. The COR will provide PS/CSO with the Risk Assessment Checklist (RAC).
b. PS/CSO will enter the RAC information into the Automated Background Investigation System (ABIS) and the Contractor Management Module.
c. PS/CSO will send the COR an Approval of Interim or Final Staff-like Access or Denial of Access memo.

(3) Federal tax compliance checks are conducted on all revalidations.

10.23.2.14.1
(04-22-2022)
Prior Staff-like Access Approval

(1) If a contractor employee was previously approved to work on an IRS contract the following applies:

a. The contractor employee can move to another IRS contract without a new investigation, if the prior investigation was completed and favorably adjudicated within the last five years and is at the same or higher level required for the current position.
b. The COR must submit a RAC to PS/CSO.
c. Final staff-like access continues, and PS will generate a revalidation of access approval letter.

(2) If a contractor employee is moving to a new contract that requires an investigation at a higher risk level, the contractor employee must have a new investigation before being granted final staff-like access on the new IRS contract.

10.23.2.15
(04-22-2022)
Re-investigation Requirements

(1) Contractor employees in positions designated as high and moderate risk will be subject to re-investigation every five years.

(2) Contractor employees in positions designated as low risk require an FBI fingerprint and a tax check every five years.

Note: The tax check is a standard reinvestigation requirement for a low risk position. However, a contractor in such position is not exempt from the periodic tax check requirement in IRM 10.23.2.2.2 (1) a.

(3) CORs are responsible for:

a. Tracking when reinvestigations are due for their contractor employees.
b. Initiating the required reinvestigation, fingerprint check, and/or tax check.
c. Submitting the RAC and other appropriate documents three months before the expiration of the most recent completed background investigation, which is five years from the investigation's close date. The reinvestigation due date is reflected in the final approval memo. A copy of the final approval memo can be obtained through the *ABIS Personnel Security*.

10.23.2.16
(04-29-2019)
Separating Contractor Employees

(1) When a contractor employee leaves the contract, the following occurs:

a. The vendor notifies the COR within one business day from the contractor employee's date of separation.
b. The COR completes the Form 14604, Contractor Separation Checklist, and forwards it to PS/CSO.
c. PS will cancel any pending investigations or adjudications and update the security file. Even if the background investigation is already completed, notification is required so that the separation information can be appropriately recorded in the security file.
d. The COR or MOR will recover the ID media on the contractor employee's last workday and return the ID media to the local FMSS security office within one workday from the separation date. Refer to IRM 10.2.5.9, Recovery of ID Media.

10.23.2.17
(05-05-2015)
Non-Disclosure Agreement (NDA) for Access to Sensitive Information

(1) IRS personnel security officers, in consultation with IRS IT systems security officers, COs, and CORs, must ensure all contractor employees requiring access to SBU information execute an NDA as a condition thereof.

10.23.2.17.1
(04-29-2019)
Execution of NDA for Access to Sensitive Information

(1) An NDA must be signed and submitted to PS/CSO prior to starting work on the contract when access to SBU information is required. When necessary, each NDA will reference to the conditional nature of access to SBU information with respect to the contract work, or specialized project, for which such access is required.

(2) The COR should use the NDA instructions/sample document provided at the *PS Contractor Forms Website*. The document has been adapted for IRS use from the non-disclosure agreement format prescribed by TD P 15-71, Chapter II, Section 2, Item 8, "Nondisclosure Agreement for Sensitive Information".

(3) The COR will provide a copy to PS/CSO along with all necessary security documents.

(4) IRS will consult with legal counsel to determine whether annual appropriations acts, in effect at the time an agreement is executed, contain provisions requiring the inclusion of specific text in NDAs.

10.23.2.17.2
(04-29-2019)
Retention of NDA for Access to Sensitive Information

(1) The original signed NDA shall be retained by the COR in the official background investigation file. For authorized disposition period, refer to Document 12990, IRS Records Control Schedule, 12 Personnel Security Records, Item 3. IRS has the discretion to maintain the agreement for as long as the information is deemed sensitive. If requested, a copy may be furnished to the individual signatory.

10.23.2.18
(05-05-2015)
Solicitations and Contracts

(1) Solicitations and contracts shall include a clause that requires position risk designations for the contractor employee, background investigation, or screening and federal tax compliance before staff-like access is granted to IRS-owned or controlled facilities, IT systems, SBU information, or security items or products.

(2) The clause shall require the successful contractor's employees to execute appropriate security forms including non-disclosure agreements (as required) prescribed by IRS PS prior to contract work being performed, and in advance of being granted staff-like access to IRS-owned or controlled facilities, IT systems, SBU information, security items or products (refer to IRM 10.23.2.2, General Investigative Requirements, IRM 10.23.2.17, Non-Disclosure Agreement (NDA) for SBU Information and TDP 15-71, Treasury Security Manual, Chapter II, Section 2, item 8, Nondisclosure Agreement for Sensitive Information).

10.23.2.19
(04-04-2008)
Protection of Personnel Security Records

(1) PII in personnel security investigations, records, and operations shall be carefully safeguarded to protect the interests of both the individual and the IRS, pursuant to requirements of the Privacy Act. Unless categorized at a higher level, or determined to be classified NSI, personnel security information must be afforded the same degree of protection as material identified as SBU as defined in IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data, 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.

(2) Personnel Security investigation information requested by the subject of an investigation must be processed according to procedures established by IRS under provisions of the Privacy Act or the Freedom of Information Act, as appropriate. Requests for the release of the results of any personnel security investigation shall be referred to the Treasury/bureau or non-Treasury agency that conducted it.

(3) Reports containing classified NSI must be protected in accordance with EO 13526, Classified National Security Information and appropriate Treasury regulations. For protection of NSI within the IRS, refer to IRM 10.9.1, Classified National Security Information .

10.23.2.20
(04-27-2016)
Advisory Committees

(1) For participants on advisory committees, pre-appointment checks are required which include a fingerprint check and tax check that is requested by the authorized IRS sponsoring official (SO). The authorized IRS SO must request the fingerprint check through PS. For more details about the appointee's screening process, refer to IRM 6.304.1, Expert and Consultant Appointments.

(2) Current IRS Advisory Committees are:

- Electronic Tax Administration Advisory Committee
- Information Reporting Program Advisory Committee
- Taxpayer Advocacy Panel
- Internal Revenue Service Advisory Council
- Tax Exempt &Government Entities
- Art Advisory Panel of the Commissioner of Internal Revenue Service

10.23.2.20.1
(04-29-2019)
Pre-Appointment Checks

(1) To conduct pre-appointment checks, the IRS SO must inform the appointee of the reasons for requesting the information, as required by the Privacy Act.

(2) Before completing the tax check and fingerprint check, the IRS SO must have the appointee read and sign Form 14767, Consent to Disclose Tax Compliance Check and Form 12333, Consent For Fingerprint Check.

a. The Form 12333 is mailed to PS and Form 14764 is maintained by the IRS SO.
b. The appointee must be fingerprinted on a SF87 or FD 258 fingerprint card or Live Scan fingerprints can be taken at limited local servicing IRS Offices or IRS approved enrollment stations.

(3) When the results of the FBI fingerprint check are completed, PS will:

a. Automatically approve any results indicating "no record".
b. Review any FBI fingerprint check with a record to determine if the applicant is suitable.
c. Document all results on an official memorandum and e-mail to the SO.

10.23.2.21
(11-15-2011)
Lockbox Employees

(1) In accordance with Wage and Investment's, Lockbox Security Guidelines, Section L.S.G.2.4.3, Employee Background Investigations, Lockbox employees must have an approved background investigation screening by IRS PS before being granted staff-like access to any lockbox facility, IT system (no matter where located), and/or sensitive data or information. Background investigations are conducted on a position risk basis as follows:

a. Full time bank employees - Appropriate investigation based on position risk.
b. Bank associates - Annual fingerprint check.
c. Temporary employees - Annual fingerprint check.

10.23.2.22
(04-22-2022)
Payment for Investigations

(1) The investigative costs for background investigations are funded by HCO.

(2) The funds for specific types of investigations will be transferred to HCO from the servicing private collection contractor/center. The SBSE organization is responsible for completing the action in the Integrated Financial System.

10.23.2.22.1
(04-22-2022)
Cancellation of Investigation

(1) PS will not bill for investigations canceled by the COR. PS must receive written notification of the cancellation from the COR within 15 calendar days from the initial request. Any investigation canceled after the 15th calendar day will be billed the current full rate.

10.23.2.23
(04-22-2022)
Security Terms and Definitions

(1) **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.

(2) **Adjudicator** - A trained personnel security specialist who evaluates background investigations and other pertinent information to make employment suitability and national security eligibility determinations.

(3) **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, i.e., drug abuse, criminal activity, employment misconduct, etc.

(4) **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.

(5) **Classified National Security Information (NSI)** - Information controlled by the U.S. Government that has been determined pursuant to EO 13526, Classified National Security Information, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(6) **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. CE leverages a set of automated record checks to assist in the assessment of an individual's continued eligibility.

(7) **Contract** - A mutually binding legal obligation or agreement for services/ supplies prepared or granted by or on behalf of the Secretary of the Treasury or a Treasury/bureau head.

(8) **Contracting Officer (CO)** - A U.S. Government official having written, designated authority to enter into, administer, and/or terminate contracts and make related determinations and findings with respect thereto on behalf of the United States government.

(9) **Contracting Officer's Representative (COR)** - An individual designated and authorized by the CO to perform contract administration activities on their behalf within the limits of delegated authority for a specific acquisition or contract.

(10) **Contractor Employee** - An individual, not a federal employee, that performs work for or on behalf of the federal government.

(11) **Contractor Employee Fitness Determination** - A fitness determination based on an individual's character and conduct to work for or on behalf of the federal government as a contractor employee.

(12) **Controlled Facility** - A designated facility, building, office where only personnel assigned to work in such areas are authorized unescorted access.

(13) **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.

(14) **Defense Information System for Security (DISS)** - A system of record for personnel security, suitability, credential management for the Department of Defense employees, military personnel, civilians, and contractors. DISS also provides secure communications between Adjudicators and Security Officers in support of eligibility and access management.

(15) **Defense Security Counterintelligence Agency (DCSA)** - Primary investigative service provider for conducting efficient and effective background investigations and continuous vetting to safeguard the integrity and trustworthiness of the federal and contractor workforce. DCSA conducts background investigations for 95% of the federal government, including 105 departments and agencies.

(16) **Escorted Access** - A contractor employee not yet granted staff-like access that needs to be accompanied by an "authorized escort" during work performance and movement throughout the facility.

(17) **Federal Tax Compliant** - Federal tax returns are timely and accurately filed and timely payment of taxes without penalties or interest.

(18) **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.

(19) **Foreign National** - An individual who is not a U.S. citizen or a LPR authorized to reside in the U.S.

(20) **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.

(21) **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.

(22) **IT Privileged Access** - Administrator or root access to DS, DSTEST and IRSNET domains that contain highly sensitive, critical information. Refer to IRM 10.23.2.5.2 for examples of DS and IRSNET domains.

(23) **Lawful Permanent Resident (LPR)** - A non-U.S. citizen who resides in the U.S. under legally recognized and lawfully recorded permanent residence as an immigrant. Also known as permanent resident alien, resident alien permit holder, and green card holder.

(24) **Lockbox Employee** - An individual employed by a commercial bank that processes financial transactions for Treasury/bureaus.

(25) **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."

(26) **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.

(27) **National Security Position** - 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 are not limited to, those requiring eligibility to classified NSI; protecting the nation from acts of terrorism, espionage, or foreign aggression; and developing plans or polices related to national defense/military operations. Refer to 5 CFR 1400, Designation of National Security Positions, Section 1400.102.

(28) **National Industrial Security Program (NISP)** – A single, integrated, cohesive industrial security program established by EO 12829 to protect federal government classified NSI that is released to contractors, licensees, and grantees of the United States Government and to preserve our Nation's economic and technological interests.

(29) **Non-Disclosure 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 Nondisclosure Agreement (SF 312) is required.

(30) **Notification of Access** - A written notice delivered to the COR and contractor employee that signifies the final staff-like access determination.

(31) **Office of Personnel Management (OPM)** - OPM is an independent federal agency that works in numerous broad areas to recruit and retain a first-rate federal workforce, which includes individuals performing work for or on behalf of the federal government.

(32) **Periodic Reinvestigation** - An investigation that is required every five years for contractor employees who perform work for or on behalf of the federal government and are in positions designated high and moderate risk.

(33) **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.

(34) **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.

(35) **Position Designation Tool (PDT)** - A logical questionnaire-based system designed by OPM to guide agencies in determining the proper level of investigation and screening required based on an assessment of risk and national security sensitivity.

(36) **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.”

(37) **Pre-screen** - A preliminary review of a security questionnaire and security checks to render an interim employment eligibility and suitability or fitness determination before initiating a background investigation.

(38) **Proposal to Deny Letter** - A written notice delivered to the contractor employee when unfavorable information is discovered during a background investigation that could adversely affect the individual’s employment suitability. The notice gives the individual the opportunity to refute, explain, clarify, or mitigate the information in question prior to PS making a final determination.

(39) **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.

(40) **Qualified Escort** - An IRS employee or a contractor employee approved for final staff-like access at the same or higher position risk level as the contractor employee who requires escorting. At least one qualified escort per every five

escorted persons is required and must accompany the escorted persons during work performance and throughout the facility. Refer to IRM 10.2.18.5.2, Escorted Access.

(41) **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.

(42) **Revalidation of Access** - Reconfirmation of a contractor employee's staff-like access when there are any material changes to a contract, a contractor employee name change, movement from one contract to another contract, or work performance on multiple contracts.

(43) **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.

(44) **Security Items** - Items that must be stored in a locked container, security container, or a secure room. These items include, but not limited to security devices/records, computer equipment, ID media. For details, refer to IRM 10.2.15, Minimum Protection Standards.

(45) **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.

(46) **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.

(47) **Staff-like Access** - Refer to IRM 10.23.2.1, Program Scope and Objectives.

(48) **Staff-like Access Denial** - An adjudicative decision to deny access based on information revealed in a background investigation, other relevant information, or both that indicates that contractor employee is not fit to perform work for or on behalf of the federal government.

(49) **Staff-like Access Revocation** - An adjudicative decision to permanently withdraw the contractor employee's staff-like access based on a background investigation, other relevant information, or both, that a cleared contractor employee is no longer fit to perform work for or on behalf of the federal government.

(50) **Subcontractor** - A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor. A subcontractor is considered a prime contractor in relation to each of its subcontractors.

(51) **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 of both parents.

(52) **Vendor** - A business or person who provides goods or services.