



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.2.18

MARCH 5, 2025

## EFFECTIVE DATE

(03-05-2025)

## PURPOSE

- (1) This transmits the revised Internal Revenue Manual (IRM) 10.2.18, *Physical Access Control (PAC)*.

## MATERIAL CHANGES

- (1) This IRM was updated to reflect current organizational titles, scope, definitions, responsibilities, and new access policy.
- (2) Throughout: Replaced references to SmartID with Personal Identity Verification (PIV) card. PIV cards are also known as credentials, common access cards, Smart cards (SmartID), badges, etc., depending on agency. PIV card is used on this IRM to be consistent with the National Institute of Standards and Technology (NIST) guidance.
- (3) Throughout: Changed the word “section” to “IRM,” when the reference refers to an IRM.
- (4) IRM 10.2.18.1.3, Roles and Responsibilities: Added note clarifying that when Human Capital Office’s (HCO) and FMSS’s IRMs are updated regarding staff-like access, it’s considered a program review.
- (5) IRM 10.2.18.1.4(3), Program Management and Review: Updated Program Reports to include documents and reports that help support the program’s objectives.
- (6) IRM 10.2.18.1.5, Program Controls: Updated controls developed to oversee the program.
- (7) IRM 10.2.18.1.6, Terms and Acronyms: Updated terms and acronyms that appear throughout this IRM.
- (8) IRM 10.2.18.1.7, Related Resources: Added IRMs 10.5.1 through 10.5.8. Removed IRM 1.4.6.
- (9) IRM 10.2.18.2, Prohibited Items:
  - a. Paragraph (1) - Updated prohibited items list per ISC Standards.
  - b. Paragraph (3) - Added procedures for requesting exceptions or exemptions and approving authorities.
- (10) IRM 10.2.18.3 (4), Screening Requirements: Updated policy on pat-down searches.
- (11) IRM 10.2.18.4 (4), Random Occupant Screening Requirements: Added Security Section Chief (SSC) or Facility Security Committee (FSC) should consider screening all “continuous” occupants during heightened security alerts, per ISC Standards.
- (12) IRM 10.2.18.6 (4), Physical Access Eligibility Requirements: Removed requirement for Physical Security Specialist to coordinate with lessor to implement Visitor Access Register requirements.
- (13) IRM 10.2.18.8 (4), Facility Access: Added Enterprise Physical Access Control System (EPACS) must be utilized as the primary method for gaining access to IRS facilities/IRS space when equipped.
- (14) IRM 10.2.18.8.3, Requesting and Granting Facility Access: Added subsection to explain procedures for requesting facility access.
- (15) IRM 10.2.18.9.1, Executive Service Employees: List of Heads of Office titles removed and replaced

with Senior Executive Services (SES). Added Senior Continuity's Representative-Continuity of Operation (SCR-CO) employees will be granted multi-facility access for their area of operation.

- (16) IRM 10.2.18.9.2 (4), Non-Executive Service Employees or Contractors: Added procedures for employee/contractors on how to get access granted while hoteling.
- (17) IRM 10.2.18.10.4 (2), Limited Area Security and Administration: Added five year retention for Form 5421, Limited Area Register.
- (18) IRM 10.2.18.10.5, Requesting and Granting Limited Area Access: Added subsection for procedures to use IRWorks to request access to Limited Areas and that the employee must be placed on the Authorized Access List (AAL) by the business unit (BU) manager if approved.
- (19) IRM 10.2.18.15 (2), Deviations: Added reference to IRM 10.2.18.2, Prohibited Items, for procedures for exceptions and exemptions to prohibited and controlled items.

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

This IRM supersedes IRM 10.2.18, dated February 3, 2023.

#### **AUDIENCE**

Servicewide

Julia W. Caldwell  
Acting Chief  
Facilities Management and Security Services

10.2.18

Physical Access Control (PAC)

## Table of Contents

10.2.18.1 Program Scope and Objectives

10.2.18.1.1 Background

10.2.18.1.2 Authority

10.2.18.1.3 Responsibilities

10.2.18.1.4 Program Management and Review

10.2.18.1.5 Program Controls

10.2.18.1.6 Terms and Acronyms

10.2.18.1.7 Related Resources

10.2.18.2 Prohibited Items

10.2.18.3 Screening Requirements

10.2.18.4 Random Occupant Screening Requirements

10.2.18.5 Vehicle Screening Requirements

10.2.18.6 Physical Access Eligibility Requirements

10.2.18.6.1 Unescorted Access

10.2.18.6.2 Escorted Access

10.2.18.7 Perimeter Access

10.2.18.8 Facility Access

10.2.18.8.1 Facility Unescorted Access

10.2.18.8.2 Facility Escorted Access

10.2.18.8.3 Requesting and Granting Facility Access

10.2.18.9 Multi-Facility Access

10.2.18.9.1 Executive Service Employees - Multi-Facility Access

10.2.18.9.2 Non-Executive Service Employees or Contractors

10.2.18.10 Limited Area Access

10.2.18.10.1 Limited Area Unescorted Access

10.2.18.10.2 Limited Area Escorted Access

10.2.18.10.3 Limited Area Access for Contracting Officer's Representatives (CORs)

10.2.18.10.4 Limited Area Security and Administration

10.2.18.10.5 Requesting and Granting Limited Area Access

10.2.18.11 Treasury Inspector General for Tax Administration (TIGTA) Access

10.2.18.12 Emergency First Responders Access

10.2.18.13 National Treasury Employees Union (NTEU) Access

10.2.18.14 Personal Assistance Services (PAS) Access

---

10.2.18.15 Deviations

10.2.18.16 Records and Accountability

10.2.18.1  
(03-05-2025)  
**Program Scope and Objectives**

- (1) This IRM section applies Physical Access Controls (PACs) to IRS facilities and space (work areas). PAC systems and procedures are designed to admit authorized personnel while simultaneously identifying and preventing unauthorized personnel entry and counter the introduction of prohibited items.
- (2) **Purpose:** This IRM establishes the framework for the application of PAC policy in IRS facilities or space (government owned or leased).
- (3) **Audience:** Servicewide.
- (4) **Policy Owner:** Chief, Facilities Management and Security Services (FMSS).
- (5) **Program Owner:** FMSS Associate Director (AD), Security.
- (6) **Primary Stakeholders:** FMSS Field Operations, Business Unit Executives, Senior Managers, Chief Counsel Executives, Managers, and Employees.

10.2.18.1.1  
(03-05-2025)  
**Background**

- (1) PACs are essential to the safeguarding of IRS personnel, tax data, and other IRS assets. PAC effectively keeps our facilities safe and secure by controlling the movement of personnel in the facility and by setting specific criteria for authorized access.
- (2) This IRM consolidates and revises all PAC policy found in IRM 10.2.1, *Physical Security*. IRM 10.2.18, *Physical Access Control (PAC)*, sets specific criteria that must be met before granting facility access. Similarly, IRM 10.23.2, *Contractor Investigations*, provides policy and describes the background investigative requirements for contractor employees (and contractor personnel) and subcontractors (and subcontractor personnel) to be granted staff-like access to IRS-owned or controlled facilities and spaces. IRMs 10.2.18 and 10.23.2, must be considered to get an overarching perspective of the entire physical access process.

10.2.18.1.2  
(03-05-2025)  
**Authority**

- (1) *Department of Homeland Security (DHS) Interagency Security Committee (ISC) Standards*
- (2) Document 12829, General Records Schedule: 5.6, Security Records
- (3) *Federal Information Processing Standards (FIPS) Publication 201*
- (4) *Federal Management Regulation (FMR) - Title 41, Code of Federal Regulations (CFR) Part 102-74 Subpart C: Facility Management - Conduct on Federal Property*
- (5) *Homeland Security Presidential Directive (HSPD)-12 - Policy for a Common Identification (ID) Standard for Federal Employees and Contractors*
- (6) *OMB Memorandum M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) -12 - Policy for a Common ID Standard for Federal Employees and Contractors*
- (7) *Title 18 United States Code (USC) Section 930, Possession of firearms and dangerous weapons in Federal facilities*
- (8) *Title 26 USC Section 6103(b), Confidentiality and disclosure of returns and return information*
- (9) *Treasury Directive Publication (TD-P) 15-71, Treasury Security Manual*

10.2.18.1.3  
(03-05-2025)  
**Responsibilities**

- (10) *Treasury Order 115-01*, Office of the Treasury Inspector General for Tax Administration
  - (1) The Chief, FMSS prescribes and is responsible for oversight of PAC policy and guidance.
  - (2) FMSS AD, Security is responsible for oversight of planning, developing, implementing, evaluating, and controlling PAC policy and guidance.
  - (3) FMSS AD, Operations and Territory Managers (TMs) are responsible to ensure Security Section Chiefs (SSCs) follow PAC policy and provide oversight in the implementation and enforcement of the program.
  - (4) FMSS SSCs are responsible for implementing and enforcing the PAC program within their assigned territory, ensuring that PAC policy and guidance are followed.
  - (5) All IRS managers, Contracting Officers (COs), Contracting Officer's Representatives (CORs), and Government Officials with personnel administrative functions have a responsibility for:
    - a. Informing all employees within their span of control of the importance of following facility PAC requirements.
    - b. Determining that only authorized personnel are in the work area for which they are responsible and immediately challenging the presence of suspected unauthorized persons.
    - c. Reporting suspected unauthorized access to the Situational Awareness Management Center (SAMC), as prescribed in IRM 10.2.8, *Incident Reporting*.
    - d. Ensuring their employees and contractor employees meet the requirements for unescorted or escorted access, to include access to Limited Areas, and to comply and enforce "qualified escort" requirements.
  - (6) All employees and contractors have a responsibility for:
    - a. Following facility PAC requirements.
    - b. Determining only authorized personnel are in the work area for which they are responsible and immediately challenging and/or reporting the presence of suspected unauthorized persons.
    - c. Reporting suspected unauthorized access to the SAMC, as prescribed in IRM 10.2.8, *Incident Reporting*.
    - d. Following unescorted or escorted access procedures, to include Limited Areas access, and comply and enforce "qualified escort" requirements, especially when designated as a "qualified escort."
  - (7) FMSS Security will collaborate with the Procurement and Human Capital Office (HCO) Personnel Security organizations to evaluate the program effectiveness related to staff-like access by contractors and subcontractors and all other non-IRS employees. Program reviews will be conducted on an as needed basis, but no less than every three years and changes will be implemented, as warranted.

10.2.18.1.4  
(03-05-2025)  
**Program Management  
and Review**

- (1) **Program Objective:** To safeguard IRS personnel, facilities, data, and other assets through the control of entry into IRS facilities.
- (2) **Program Goals:** To provide policy and guidance designed to admit only authorized persons into IRS facilities.
- (3) **Program Reports:** The PAC program reports include:
  - a. Access Control Records - A set of documents that record physical access data and is reviewed as necessary.
  - b. Authorized Access List (AAL) - A list of individuals who have a frequent and continuing need to enter a Limited Area, prepared monthly by the Limited Area manager.
  - c. Form 5421, *Limited Area Register (LAR)* - An official form that records entry into a Limited Area, verified monthly by a Limited Area front-line supervisor to ensure only authorized visitors have access to IRS limited areas.
  - d. SAMC Incident Reports - A report of physical security incidents and/or threats.
  - e. Visitor Access Register (VAR) - A daily record of visitors entering a facility, maintained by FMSS Physical Security Staff to document visitor's access to the facility.
- (4) **Program Effectiveness:** PAC program reviews will be utilized to assess the effectiveness of the physical access controls. This review is conducted on an as-needed basis and as determined by AD, Security and provides access control information based on the program manager's oversight activities.
- (5) **Program Review:** FMSS AD, Security conducts review of all PAC program policies and guidance as needed and makes appropriate updates.

10.2.18.1.5  
(03-05-2025)  
**Program Controls**

- (1) Analysis of physical access related SAMC reports, Facility Security Assessments (FSA) findings, and Facility Security Compliance Assessments (FSCA) recommendations.
- (2) Management maintains continuous oversight of projects and program activities through regular project status meetings and status reporting.

10.2.18.1.6  
(03-05-2025)  
**Terms and Acronyms**

- (1) **Access** - The authority granted to employees, contractors, and visitors that provides opportunity to physically come into contact with (including, but not limited to reading, transporting, and/or transcribing/interpreting) Sensitive But Unclassified (SBU) data in the performance of official duties, entering an IRS facility without escort, and/or to login to IRS systems with approved credentials.

**Note:** For additional information, refer to IRM 10.23.1, *National Security Positions and Classified Information*, and IRM 10.23.2, *Contractor Investigations*.

- (2) **Access Control** - Procedures designed to admit authorized personnel and prevent entry by unauthorized persons.
- (3) **Authorized Access List (AAL)** - A list of persons approved by the assigned FMSS Physical Security Staff for unescorted or escorted physical access. Also used in Limited Areas to identify persons approved by the business unit manager/supervisor for unescorted access into designated Limited Areas.

- (4) **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.
- (5) **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.

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

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

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

- (7) **Controlled Items** - Potentially dangerous devices or items that are not prohibited in federal facilities but may require advance notification for entry for federal and contract employees only. Visitors cannot bring controlled items into a federal facility.
- (8) **Employee** - A federal employee, employed by the IRS.
- (9) **Enterprise Physical Access Control System (EPACS)** - IRS system to physically grant access to a specific area.
- (10) **Escorted Access** - A situation where an individual (i.e., employee, contractor employee, visitor, or vendor) who is not approved for staff-like access and therefore must be accompanied by a "qualified escort" during work performance and movement throughout the facility.

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

- (11) **Exceptions** - A new or modification of existing PAC policy, temporary in nature and granted for specific occurrences or a defined period.
- (12) **Exemptions** - A new or modification of existing PAC policy, are permanent in nature until rescinded.
- (13) **Facility Access** - Controlled entry into a facility based on access status, role or function, and employment category.
- (14) **Facility Security Committee (FSC)** - A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities.
- (15) **Limited Area** - An area to which access is limited to authorized personnel only and requires a two-factor authentication mechanism to gain access.

**Note:** For additional information, refer to IRM 10.2.14, *Methods of Providing Protection*.

- (16) **Perimeter Access** - Pedestrian and/or vehicular access to controlled exterior areas, marked by a fence or a similar boundary marking, usually at campus locations.



- (17) **Perimeter Vehicle Access Register (PVAR)** - Daily record of vehicles, without passes, entering the perimeter.
- (18) **Personal Identity Verification (PIV) Card** – A federal government-issued identification card that allows access to secured facilities and information systems. PIV cards are also known as credentials, common access cards, smart card (smartID), badges, etc. depending on agency. “PIV card” is used on this IRM to be consistent with the National Institute of Standards and Technology (NIST) guidance.
- (19) **Prohibited Items** - An item, legal or illegal in nature, where possession is restricted from entry into a facility by federal, state or local law, regulation, court-order, rule, or FSC policy.
- (20) **Qualified Escort** - An authorized (designated) IRS employee or a contractor employee approved for final staff-like access at the same or higher position risk level as the contractor employee or visitor who requires escorting, and with knowledge of the task or activity to be performed.

**Note:** For additional information on escort/escorted ratio, refer to IRM 10.2.18.6.2, *Escorted Access*.

- (21) **Routine Access** - Access to facilities on a consistent basis, generally multiple times a week; however, telework agreements and Procurement contracts may establish a lengthier frequency (e.g., bi-weekly or bi-monthly).
- (22) **Security Organization** - The government agency or an internal agency component either identified by statute, interagency memorandum of understanding/memorandum of agreement, or policy responsible for physical security for the specific facility and performs preliminary Facility Security Level (FSL) determinations and initial or recurring risk assessments.
- (23) **Staff-like Access** - Authorized unescorted access to IRS-owned or controlled facilities, Information Technology (IT) systems, security items and products, and/or to areas storing/processing SBU data, as determined by Treasury/bureau officials. Staff-like access may be interim or final.

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

- (24) **Unescorted Access** - Staff-like access granted to a contractor employee to IRS facilities, IT systems, and SBU data without escort.

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

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

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

- (26) **Visitor** - A person visiting an IRS facility who has not been issued an IRS identification (ID) card. Visitors may include contractors who have or have not been approved for staff-like access, other federal agency employees and contractors, and the general public.
- (27) **Visitor Access Register (VAR)** - Daily record of visitors entering the perimeter or the facility.

**Acronyms**

<b>Acronym</b>	<b>Definition</b>
AAL	Authorized Access List
AD	Associate Director
BB	Ball Bearing
BOD	Business Operating Division
BU	Business Unit
CFR	Code of Federal Regulations
CO	Contracting Officer
COR	Contracting Officer's Representative
CSR	Contractor Separation Report
DHS	Department of Homeland Security
EPACS	Enterprise Physical Access Control System
EEOC	Equal Employment Opportunity Commission
FAST	Field Assistance Scheduling Tool
FIPS	Federal Information Processing Standards
FMR	Federal Management Regulation
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
FSA	Facility Security Assessment
FSC	Facility Security Committee
FSCA	Facility Security Compliance Assessment
FSL	Facility Security Level
HCO	Human Capital Office
HSPD	Homeland Security Presidential Directive
ID	Identification
IG	Inspector General
ISC	Interagency Security Committee
IT	Information Technology
LAR	Limited Area Register

Acronym	Definition
NTEU	National Treasury Employees Union
NWDTP	National Weapons and Detection Program
OEP	Occupant Emergency Plan
PAC	Physical Access Control
PAS	Personal Assistance Services
PIV	Personal Identity Verification
POC	Point of Contact
PSO	Protective Security Officer
PVAR	Perimeter Vehicle Access Register
ROS	Random Occupant Screening
SAMC	Situational Awareness Management Center
SAT	Security Awareness Training
SEC	Separating Employee Clearance
SBU	Sensitive But Unclassified
SSC	Security Section Chief
TAC	Taxpayer Assistance Centers
TDP	Treasury Department Publication
TIGTA	Treasury Inspector General for Tax Administration
TM	Territory Manager(s)
VAR	Visitor Access Register
VGSA	Visitor Group Security Agreement

10.2.18.1.7  
(03-05-2025)

#### Related Resources

- (1) IRM 10.2.5, *Identification Media*
- (2) IRM 10.2.8, *Incident Reporting*
- (3) IRM 10.2.14, *Methods of Providing Protection*
- (4) IRM 10.5.1, *Privacy Policy*
- (5) IRM 10.5.2, *Privacy Compliance and Assurance (PCA) Program*
- (6) IRM 10.5.4, *Incident Management Program*

- (7) IRM 10.5.5, *IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements*
- (8) IRM 10.5.6, *Privacy Act*
- (9) IRM 10.5.7, *Use of Pseudonyms by IRS Employees*
- (10) IRM 10.5.8, *Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments*
- (11) IRM 10.8.1, *Information Technology (IT) Security, Security Policy*
- (12) IRM 10.23.1, *National Security Positions and Access to Classified Information*
- (13) IRM 10.23.2, *Contractor Investigations*

10.2.18.2  
(03-05-2025)  
**Prohibited Items**

- (1) IRS employees, contractors, visitors, and the general public are not permitted to enter IRS facilities and/or space with items prohibited in Federal Management Regulation (FMR) - *Title 41 CFR*, unless specifically authorized by *18 USC 930*. Prohibited items include but are not limited to:
  - a. Any item prohibited by any applicable federal, state, local, and tribal law and/or ordinance.
  - b. Firearms or projectiles - Ball bearing (BB) or pellet guns, compressed air guns, antique firearms, flare guns, ammunition, or replica weapons.
  - c. Knives or other bladed devices with blades in excess of 2.5 inches - Swords, axes, throwing stars, bow and arrows.
  - d. Club-like or striking devices - Night sticks, brass knuckles, nun chucks, batons
  - e. Dangerous devices - Explosives or combustibles, fireworks, gunpowder, blasting caps, or realistic explosive replicas.
  - f. Disabling chemicals - Mace, pepper spray, tear gas.
  - g. Other destructive devices (including their individual parts or components) designed, redesigned, used, intended for use, or readily converted to cause injury, death, or property damage.
- (2) IRS employees, contractors, visitors, and the general public will be denied access if they attempt to enter a facility with prohibited items.
- (3) In certain circumstances, the assigned FMSS Physical Security Staff may request exceptions or exemptions to the list of prohibited items at a facility, in accordance with guidance outlined in the ISC document, *Items Prohibited from Federal Facilities: An Interagency Security Committee Standard*.
  - a. Facility occupants requesting authorization to enter with or possess a prohibited or controlled item (tools, sports equipment, training aids, etc.), must do so in accordance with ISC Standard guidelines, prior to entry into the facility.
  - b. For prohibited items, the Operations Area AD is the approving authority for exceptions and exemptions.
  - c. For controlled items, the Territory Manager is the approving authority for exceptions and exemptions.
  - d. When there is an approved facility-specific list of prohibited items, it must be reviewed annually in conjunction with the Facility Security Plan (FSP).
  - e. For multi-tenant facilities, when IRS chairs the Facility Security Committee (FSC), the Chair will ensure the security organization is

- provided copies of all approved exceptions and exemptions of prohibited items for distribution to screening checkpoints and staff, as appropriate.
- f. For sole-tenant facilities, the FMSS Physical Security Staff will provide copies of approved exceptions and exemptions of prohibited items to the security organization and screening checkpoints.
- g. Per ISC guidance, a notice of prohibited items should be posted at each public entrance to the facility.

10.2.18.3  
(03-05-2025)  
**Screening Requirements**

- (1) Employees, contractors, visitors, and the general public may be subjected to screening of personal effects at facility entrance(s) to deter and detect prohibited items. Screening requirements are in accordance with current ISC Standards and may vary by location.
- (2) Packages of all types (including luggage, briefcases, shoulder bags, athletic bags, and handbags) are subject to screening. Inspection includes opening the item and viewing its contents and/or viewing x-ray images of the item to determine if unauthorized items are present.
- (3) Facility entrants may request alternative screening methods. **Personnel with a “pacemaker” may be screened with hand-held metal detectors or hand wands per Federal Protective Service (FPS) National Weapons and Detection Program (NWDTP).** All persons declaring a medical condition which prohibits them from metal detection screening must submit to alternative methods of screening. No proof of medical condition is required.
- (4) FPS is responsible for considering and implementing alternative methods of screening personnel. Alternative screening methods may include but are not limited to the following:
  - a. Removal of outerwear clothing (coat, jacket, sweater, etc.) for visual inspection.
  - b. Pat-down searches by Protective Security Officers (PSO) if items not removed cannot be observed.

**Note:** PSO have special instructions on how to conduct pat-down searches which must be conducted in a professional and respectful manner - consistent with security needs, agency policy, and in the least intrusive manner possible - including consideration of officer safety.
  - c. Removal of all personal belongings from pockets/person for x-ray screening or visual inspection.
  - d. Other optional and reasonable screening methodology, per local procedures.
- (5) Requests for modifications to entry access screening requirements must be submitted by the assigned FMSS Physical Security Staff to the FMSS AD, Security for coordination and approval. Modification requests should include identified risk(s) and appropriate mitigation strategies to address the risk.

**Note:** For additional information, refer to IRM 10.2.18.15, *Deviations*.

- 10.2.18.4  
(03-05-2025)  
**Random Occupant Screening Requirements**
- (1) Random Occupant Screening (ROS) is an integral part of physical security that contributes to IRS facilities' overall security posture.
  - (2) ROS of all occupants will be conducted in facilities that meet all four criteria below:
    - a. At IRS Facility Security Level (FSL) III-V facilities (owned or leased)
    - b. When IRS is the sole tenant
    - c. When PSOs and screening equipment are present
    - d. In accordance with FPS policy and ISC Standards
  - (3) SSCs must coordinate with FPS to ensure that ROS is implemented and conducted in accordance with ISC Standards.
  - (4) During a heightened security alert, the FSC or SSC should consider screening all "continuous" occupants.
- 10.2.18.5  
(03-05-2025)  
**Vehicle Screening Requirements**
- (1) SSCs coordinate with FPS to conduct vehicle screening in accordance with ISC Standards.
- 10.2.18.6  
(03-05-2025)  
**Physical Access Eligibility Requirements**
- (1) Access to IRS facilities and work areas is provided to IRS employees, contractors, and visitors on an escorted or unescorted basis. The assigned FMSS Physical Security Staff will determine and grant the type of access, based on the eligibility requirements.
  - (2) The requirements for unescorted and escorted access are set forth in IRM 10.2.18.6, *Physical Access Eligibility Requirements*, IRM 10.23.2, *Contractor Investigations*, and IRM 10.8.1, *Information Technology (IT) Security, Security Policy*.
  - (3) A daily Visitor Access Register (VAR) approved by the assigned FMSS Physical Security Staff, must be used to verify a visitor's eligibility for:
    - a. Unescorted access when they do not possess an IRS Personal Identification Verification (PIV) card.  
**Note:** For additional information, refer to IRM 10.2.18.8.1, *Facility Unescorted Access*.
    - b. Escorted access.
  - (4) VAR is used at IRS facilities (owned or leased) where the IRS is the sole tenant and responsible for controlling access using PSO services. Upon identification of a valid need for facility access and appropriate identification, the PSO will document access in the VAR.
    - a. At multi-tenant facilities, the FSC will make the VAR use determination, in consultation with the FSC IRS representative, and the security organization responsible for the facility.
    - b. IRS facilities dedicated solely to Taxpayer Assistance Centers (TAC) operations are exempt from VAR requirements.
    - c. FSL/VAR matrix:

FSL	Condition	Procedure
III, IV, and V	IRS sole tenant and security guard services control facility access	Use VAR as prescribed in IRM 10.2.18
I thru V	Multi-tenant facility	FSC determination as prescribed in IRM 10.2.18
I, II, and III	Lessor controls facility access using security guard services	Assigned FMSS Physical Security Staff or designee coordinates with lessor to possibly implement VAR
TAC	Locations without security guard services	VAR is not required. Note: TAC taxpayer or visitor tracking, if required, will be conducted as per TAC guidance and/or via the Field Assistance Scheduling Tool (FAST)

**Note:** Contact your Territory SSC for other scenarios not covered by the FSL/VAR Matrix.

- (5) Territories are authorized to create and publish a VAR to address unique requirements; however, VAR must contain at minimum, the following information:
  - a. Name, telephone number, and location of IRS Point of Contact (POC)
  - b. Visitor name and contact information
  - c. Reason for visit
  - d. Rooms/Areas to be visited
  - e. Actual date(s) and times of visit
  - f. Type of access to be granted; unescorted or escorted
  - g. Escort's full name
- (6) The VAR must be checked and validated during the review of the Separating Employee Clearance (SEC) report and the Contractor Separation Report (CSR).
  - a. Individuals who no longer require access, including names on SEC and CSR reports, must be validated and removed from the VAR by the assigned FMSS Physical Security Staff.

10.2.18.6.1  
(02-03-2023)  
**Unescorted Access**

- (1) Unescorted access allows for staff-like facility access, with the exception of designated Limited Areas. Unescorted access is provided to all IRS employees.



- (2) IRS contractors, other federal agency employees and contractors, and other persons requiring routine access must meet the following requirements before unescorted facility access is granted:
  - a. An adjudicated favorable background investigation.
  - b. Interim or final staff-like access approval from HCO Personnel Security, as set forth in IRM 10.23.2, *Contractor Investigations*.
  - c. Documented completion of designated Security Awareness Training (SAT) as set forth in IRM 10.8.1, *Information Technology (IT) Security, Security Policy*.
  - d. An established need for entry and meet the “routine access” definition of this IRM.

10.2.18.6.2  
(02-03-2023)

#### **Escorted Access**

- (1) Escorted access does not allow for the entry and/or movement throughout the facility without a “qualified escort.” Limited Areas may be subject to more stringent escort access procedures, as determined by SSCs in coordination with the Limited Area manager/supervisor.
- (2) IRS contractors, other federal agency employees and contractors, and other persons requiring routine access that do not meet the requirements for unescorted access must be escorted at all times while in IRS facilities.
- (3) A “qualified escort” will be required for persons with escorted access. The requirements for a qualified escort are as follows:
  - a. Must be only authorized (designated) IRS or contractor employees approved for final staff-like access at the same or higher position risk level as the escorted person, with knowledge of the task or activity to be performed.
  - b. Must accompany the person during all work performance and movement throughout the facility.
  - c. Must, at a minimum, maintain visual contact with the escorted person.
  - d. Must accompany visitors to the exit on completion of the visit to sign out and return any identification media issued.

**Note:** Persons who have been denied final staff-like access cannot be escorted.

- e. At no time during escorted access are individuals permitted access to SBU data, or IRS IT systems.

**Note:** For additional information, refer to IRM 10.23.2, *Contractor Investigations*.

- (4) The FMSS AD, Security is the approval authority for exception of the escort/ escorted ratio requirements:
  - a. At least one qualified escort per every five escorted persons is required.
  - b. The total number of escorts may depend on the size of the group.
  - c. The number of escorts required should be noted in the Visitor Group Security Agreement (VGSA), Contract Agreement, or similar document.
  - d. The business unit (BU) sponsoring the escorted individual(s) is responsible for providing qualified escort(s). Similarly, BU managers are responsible for ensuring their designated escort(s) meet qualified escort requirements.



10.2.18.7  
(03-05-2025)  
**Perimeter Access**

- (1) Perimeter access is controlled at locations where the IRS is responsible for perimeter security and includes pedestrian and vehicular access.
- (2) Employees and contractors that have an IRS issued PIV card and/or additional ID media, such as parking permits and/or facility access cards, must present the ID card and other media at the entry point to gain access to the perimeter area.
- (3) Employees and contractors that do not possess a parking permit and/or facility access cards, visitors, and delivery personnel may only enter at staffed perimeter entry/checkpoints. Vehicle passes, logs, and a VAR can be used to authorize perimeter access, vehicular or pedestrian. The persons will be required to provide valid photo ID, such as a driver's license, for identify verification and are subject to local screening procedures.
- (4) Temporary vehicle passes may be issued to employees, contractors, and visitors who have not been issued a parking permit.
- (5) A Perimeter Vehicle Access Register (PVAR) will be maintained by the guard and must include the following information:
  - a. Vehicle pass number
  - b. Name of driver
  - c. Vehicle license number
  - d. Pass date of issue/expiration
- (6) Territories are authorized to create and publish a PVAR to address unique requirements; however, the PVAR must contain the elements notated in this subsection paragraph (5).
- (7) The temporary vehicle pass may not be used for in and out access, but rather the visitor must show a picture ID and be checked against the VAR each time the visitor enters. A temporary vehicle pass must be dated and is valid only for the date of issuance.

10.2.18.8  
(03-05-2025)  
**Facility Access**

- (1) Facility access refers to controlled entry into a facility based on access status, role or function and employment category. Facilities may include federal buildings and commercial leased locations. Only authorized personnel should have unescorted access to IRS facilities.
- (2) To prevent unauthorized access and use of fraudulent identification cards at facilities with PSOs during ROS or heightened security alerts, or when the Enterprise Physical Access Control System (EPACS) is not installed or inoperative, assigned PSOs will:
  - a. Physically touch the ID
  - b. Compare the individual's face to the photo on the ID
  - c. Verify the card is not expired
  - d. Verify the accuracy of the other data elements printed on the card
  - e. Visually check the card security feature(s)
- (3) ID cards must be worn between the neck and waist and displayed visibly from the front when in IRS facilities/IRS space.
- (4) Facilities equipped with EPACS must utilize this system as the primary method for gaining access to IRS facilities/IRS space. It is crucial to avoid using mechanical keys to bypass EPACS, as electronic access is employed, for

example, to determine who is present within a facility during emergencies and to strengthen the Insider Threat Program.

10.2.18.8.1  
(03-05-2025)  
**Facility Unescorted Access**

- (1) Only employees, IRS contractors, other federal agency employees and contractors, that meet the eligibility requirements as outlined in IRM 10.2.18.6.1, *Unescorted Access*, are permitted unescorted access to IRS facilities.
- (2) Contractors, meeting the unescorted access requirements that do not have an IRS issued PIV card may be placed on a VAR, approved by the assigned FMSS Physical Security Staff.
- (3) Assigned FMSS Physical Security Staff will determine if additional ID media may be required.
- (4) Employees and contractors must ensure that only authorized personnel are in the workspace.

**Note:** Do not allow persons to follow behind (also known as “tailgating” or “piggy-backing”) when entering the workspace or facility.

10.2.18.8.2  
(02-03-2023)  
**Facility Escorted Access**

- (1) IRS contractors, other federal agency employees and contractors, and visitors that do not meet the requirements for unescorted access must be escorted at all times while in IRS facilities and workspace. Escorted access does not allow for the entry and/or movement throughout the facility without a qualified escort.
- (2) Escorted persons will require a qualified escort. Refer to IRM 10.2.18.6.2, *Escorted Access*, for the requirements for qualified escort(s).

10.2.18.8.3  
(03-05-2025)  
**Requesting and Granting Facility Access**

- (1) General facility access to the individual's post of duty (POD) will be granted after a Discovery Directory validation and during ID card/PIV issuance.
- (2) All requests for access to additional facilities and BU-specific area access will be handled via IRS Service Central (IRWorks) Facility Access Application.
- (3) The IRS sponsor of visitors, as defined in this IRM, must utilize IRS Service Central (IRWorks) Visitor Access Application to request access.
- (4) For facilities without EPACS, that are utilizing key/lock or cipher lock (combination) for granting facility access, the employee or contractor must contact the local FMSS Physical Security Staff for procedures to request key(s) or combination(s).

**Note:** Refer to IRM 10.2.14, *Methods of Providing Protection*, for guidance for issuing, controlling, and safeguarding of facility perimeter access door keys, limited and critical area door keys, master keys, and cipher lock combinations.

10.2.18.9  
(02-03-2023)  
**Multi-Facility Access**

- (1) The assigned FMSS Physical Security Staff has final multi-facility access acceptance or denial authority.

10.2.18.9.1  
(03-05-2025)

**Executive Service  
Employees -  
Multi-Facility Access**

- (1) Senior Executive Service (SES) employees, Heads of Office, will be granted multi-facility or nation-wide facility access as required.
- (2) Senior Continuity Representative-Continuity of Operation (SCR-CO) employees will be granted multi-facility access for their area of operation.

10.2.18.9.2  
(03-05-2025)

**Non-Executive Service  
Employees or  
Contractors**

- (1) Multi-facility access is considered and approved on a case-by-case basis and must meet the following requirements:
  - a. Personnel must meet the access requirements stated in IRM 10.2.18.6, *Physical Access Eligibility Requirements*.
  - b. Secure approval of the manager or COR.
  - c. Access can be supported by EPACS.
- (2) Employees or contractors must contact the assigned FMSS Physical Security Staff to find out the procedures for gaining access to a facility that is not their assigned POD.
- (3) For facilities without EPACS, that are utilizing key/lock or cipher lock (combination) for facility access, the employee or contractor must contact the assigned FMSS Physical Security Staff to find out the procedures to request key(s) or combination(s).
- (4) A workspace reservation (hoteling) does not grant access to the building or IRS office space. The employee or contractor must contact the local FMSS Physical Security Staff to determine the process for gaining access while hoteling.
- (5) Employee or contractor lists/rosters are not an authorized document (source) to grant multi-facility access.

10.2.18.10  
(02-03-2023)

**Limited Area Access**

- (1) A Limited Area is an area to which access is limited to authorized personnel only and requires a two-factor authentication mechanism to gain access as described in IRM 10.2.14, *Methods of Providing Protection*. Access, unescorted or escorted, must be approved by the BU manager/supervisor responsible for the area.
- (2) Visitors will be directed to the main entrance of the Limited Area for entry.

10.2.18.10.1  
(03-05-2025)

**Limited Area Unescorted  
Access**

- (1) Unescorted access allows for staff-like (unsupervised) access to designated Limited Areas and is provided to personnel:
  - a. Meeting facility unescorted access requirements.
  - b. Approved by the BU manager/supervisor responsible for the area.
  - c. Possessing a PIV card with an "R" indicator.
  - d. Placed on a designated Authorized Access List (AAL) for the Limited Area.

**Note:** The BU supervisor is a front-line manager that is delegated, by the business operating division (BOD) or department-level manager, with the daily supervision of the activities in a Limited Area. The front-line manager is also known as the "Limited Area Manager."

- (2) Personnel on an AAL will not be required to sign-in nor will the Limited Area Monitor be required to make any entry in the Limited Area Register (LAR).

**Note:** Refer to IRM 10.2.18.10.4, *Limited Area Security and Administration*, for Limited Area Monitor responsibilities.

- (3) Identity verification and a signature will be required for issuance of a temporary access card to the Limited Area.

10.2.18.10.2  
(03-05-2025)

**Limited Area Escorted Access**

- (1) Limited Area escorted access does not allow for the entry and/or movement throughout the designated Limited Area without a qualified escort. Escorted access applies to individuals who must perform official duties within Limited Areas and have not been granted unescorted entry authorization. Escorted access also applies to personnel visiting Limited Areas, and IRS employees possessing a PIV card without an "R" indicator and not listed on the AAL.
- (2) IRS contractors, other federal agency employees and contractors that do not meet the requirements for staff-like access must be escorted at all times while in designated Limited Areas.
- (3) At the main entrance of an occupied/staffed Limited Area, a Limited Area Monitor (BU staff or receptionist) will be posted and will:
  - a. Complete the Form 5421, *Limited Area Register*, for each visitor and have the visitor sign the register.
  - b. Verify the identity of each visitor by comparing the name and signature entered on the register with the name and signature on a government issued photo ID card (i.e., driver's license).
  - c. Issue a Limited Area ID card after confirming the individual's identity. If the visitor is an IRS employee or IRS contractor not assigned to the Limited Area, they must exchange an identification document, such as a driver's license or another ID that is compliant with the *REAL ID Act of 2005*, for the Limited Area ID card.

**Note:** The PIV, as a controlled item, must not be used in temporary badge issuance exchanges, per TD P 15-71, Chapter 6: Physical Security.

  - d. Collect the Limited Area ID card and return the visitor's ID card from visitors leaving the areas.
  - e. Enter visitor's time of departure (Time Out) in the register.
- (4) A qualified escort will be required for persons with escorted access.

10.2.18.10.3  
(02-03-2023)

**Limited Area Access for Contracting Officer's Representatives (CORs)**

- (1) CORs who have responsibility for programs and operations within a Limited Area, are authorized access to the Limited Area where their employees and/or contractors would be performing work. This enables the oversight and management of employees, contractors, and processes to include unannounced site visits and inspections.
- (2) CORs must meet the requirements for Limited Area unescorted or escorted access before entering the Limited Area.

10.2.18.10.4  
(03-05-2025)

**Limited Area Security and Administration**

- (1) BUs are responsible for the security and administration of their respective Limited Area(s). Limited Area administration will include the management of the documents and procedures covered in (2) thru (5).

- (2) Form 5421, *Limited Area Register*, will be closed out at the end of each month, reviewed by the Limited Area front-line supervisor, and forwarded to the Limited Area Manager. The Limited Area Manager will review the register and retain it for at least five years, but longer retention is authorized if required for business use. The managerial review is designed to ensure that only authorized individuals with an official need, have access to the Limited Areas.
- (3) The Authorized Access List (AAL) must be maintained to facilitate the entry of employees who have a frequent and continuing need to enter a Limited Area.
  - a. The BU manager/supervisor responsible for the Limited Area must approve all names added to the AAL.
  - b. The AAL will be prepared monthly and will be dated and signed by the manager. Before signing the AAL, the manager must validate the need of individuals to access the Limited Area.
  - c. The manager must sign and date the list for validation, even when there are no changes to the list.
  - d. At the end of each month the manager will review the AAL and the LAR and forward a copy to the assigned FMSS Physical Security Staff for review and identify changes required to modify ID media/access as appropriate.
  - e. The BU manager/supervisor responsible for the Limited Area must maintain the original AAL and LAR.
  - f. Only copies of the forms are authorized to be distributed to those with an official need to know.
- (4) Limited Area Monitors (BU staff or Receptionist) Requirements - Authorized Personnel:
  - a. **Entrances that are equipped with card readers** - Each individual who is authorized to enter the area is required to use their card and PIN (if required) to unlock the door every time they enter the Limited Area. During periods of unacceptable backups, due to excess traffic or system breakdowns, monitors and/or supervisors must control entrances for Limited Areas when card readers and/or PINs cannot be used, per local procedures.
  - b. **Entrances without card readers** - Authorized individuals must display their PIV card to the monitor each time they enter the area.
  - c. **Lost or forgotten PIV cards** - Use escorted access procedures until PIV card is found or re-issued.
  - d. The monitor maintains an AAL for all personnel whose PIV cards are not coded for the Limited Area, but who are authorized unescorted access to the Limited Area. Only the applicable BU manager, or their designated representative, can add a name to this AAL and it must be done in writing.

**Note:** Visits to the Limited Area by AAL personnel do not need to be recorded on the LAR.
- (5) Limited Area Monitors (BU staff or Receptionist) Requirements - Visitors. The Limited Area monitor will:
  - a. Process all visitors who need to enter the Limited Area per IRM 10.2.18.10.2, *Limited Area Escorted Access*.
  - b. Record visitors to the Limited Area on the Form 5421, *Limited Area Register*.

c. Issue a Limited Area (Visitor Escort Only) access card as required.

10.2.18.10.5  
(03-05-2025)

**Requesting and  
Granting Limited Area  
Access**

- (1) Limited Area access requests must be submitted via the IRS Service Central (IRWorks) Facility Access application.
- (2) The BU manager/supervisor or designee responsible for the Limited Area must add the employee or contractor to the AAL for the Limited Area.

10.2.18.11  
(03-05-2025)

**Treasury Inspector  
General for Tax  
Administration (TIGTA)  
Access**

- (1) TIGTA employees will be granted staff-like access, consistent with IRS security access policy, to IRS facilities when they present their PIV card at facility entry points. TIGTA employees entering IRS facilities without their PIV card are subject to the escorted access requirements as outlined in IRM 10.2.18.6.2, *Escorted Access*.
- (2) TIGTA, under Treasury Order 115-01 and 26 USC 6103(b) and while executing the functions of TIGTA, is authorized access to all facilities of the IRS and related entities, including computer facilities and computer rooms, electronic data bases and files, electronic and paper records, reports and documents, and other material available to the IRS related entities which relate to their programs and operations; and, when access is necessary to execute a function of the Inspector General (IG) pertaining to a matter within the jurisdiction of the IG, all similar facilities and material throughout the department.

10.2.18.12  
(07-05-2018)

**Emergency First  
Responders Access**

- (1) Federal and/or local emergency responders may be allowed unescorted access when responding to known emergency event (i.e., alarm activations, 911 call, or notification by the Occupant Emergency Plan (OEP) team).
- (2) For non-emergency events, emergency responders must be escorted at all times.

10.2.18.13  
(02-03-2023)

**National Treasury  
Employees Union  
(NTEU) Access**

- (1) NTEU Chapter Presidents who meet the access eligibility requirements for staff-like access will be granted access to IRS facilities consistent with IRS security access policy. NTEU Chapter Presidents will be granted access to their assigned facility where their office is located - comparable to the IRS POD term. However, they may be eligible for multi-facility access, on a case-by-case basis, and after meeting access requirements.
- (2) IRS retirees serving as stewards are subject to all security policies and procedures applicable to visitors entering IRS facilities or workspaces.
- (3) NTEU Representatives certified or sponsored by the Union's National Office, with reasonable advance notice, may visit the cafeterias or other non-work areas located in the facility's public areas to discuss Union-business with individuals or small groups of employees who are members of the bargaining unit. Such representatives must comply with all IRS security requirements and access to the facility.

10.2.18.14  
(03-05-2025)

**Personal Assistance  
Services (PAS) Access**

- (1) On January 3, 2017, the Equal Employment Opportunity Commission (EEOC or Commission) amended the regulations implementing Section 501 of the Rehabilitation Act of 1973, the law that prohibits the federal government from discriminating in employment based on disability and requires it to engage in affirmative action for people with disabilities. As part of the agencies' obligation to engage in affirmative action, federal agencies are required by the new regu-



lations to provide access to Personal Assistance Services (PAS) personnel for individuals who need them because of certain disabilities.

**Note:** Refer to 29 CFR 1614.203(d)(5)(i).

- (2) This paragraph stipulates the requirements for access control for PAS personnel for IRS employees with disabilities, who have access and functional needs and require PAS to maintain their usual level of independence in IRS facilities or space. The requirements ensure that PAS personnel entering, working within, or exiting IRS facilities or space have been granted authority to be inside the facility, are positively identified prior to entering, and accounted for as necessary. This policy includes individuals or devices that assist a person with a physical, sensory, mental, or learning disability.
  - a. PAS unescorted access will be consistent with IRM 10.2.18.6.1, *Unescorted Access*.
  - b. PAS escorted access will be consistent with IRM 10.2.18.6.2, *Escorted Access*.

10.2.18.15  
(03-05-2025)  
**Deviations**

- (1) Requests for the development of new or modification of the existing PAC policy, must be submitted through the assigned FMSS Physical Security Staff to the FMSS AD, Security, for coordination and approval.
- (2) Refer to IRM 10.2.18.2, *Prohibited Items*, for procedures for exceptions and exemptions to prohibited and controlled items.

10.2.18.16  
(07-05-2018)  
**Records and Accountability**

- (1) The assigned FMSS Physical Security Staff will be responsible for maintaining VAR and PVAR for a period of five years for areas designated as FSL V, and for two years for areas designated as FSL I through IV, and then destroy according to the *General Records Schedule 5.6, Security Records, Item 110 and 111*.

