MANUAL TRANSMITTAL

10.2.18

Department of the Treasury
Internal Revenue Service

FEBRUARY 3, 2023

EFFECTIVE DATE

(02-03-2023)

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) The following sections have been updated/clarified/added with this version of policy:

a. IRM 10.2.18.3, Screening Requirements updated to include alternative screening methods.
b. IRM 10.2.18.4, Random Security Inspections changed to Random Occupant Screenings (ROS).
c. Added subsection IRM 10.2.18.5, Vehicle Screening Requirements.
d. Added subsection IRM 10.2.18.9, Multi-Facility Access.
e. Added subsection 10.2.18.10.3, Limited Area Access for Contracting Officer's Representative (COR).
f. Added subsection 10.2.18.10.4, Limited Area Security and Administration.
g. Clarified IRM 10.2.18.11, Treasury Inspector General for Tax Administration (TIGTA) Access.
h. Added subsection IRM 10.2.18.13, National Treasury Employees Union (NTEU) Officers Access.
i. Added subsection IRM 10.2.18.14, Personal Assistance Services (PAS) Access.

(3) This document is substantially revised and must be completely reviewed.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.2.18, dated July 5, 2018.
This IRM incorporates Interim Guidance FMSS-10-0222-0002, dated March 15, 2022.
This IRM incorporates Interim Guidance FMSS-10-0422-0003, dated May 19, 2022.
This IRM incorporates Interim Guidance FMSS-10-0922-0006, dated October 31, 2022.

AUDIENCE

Servicewide

Richard L. Rodriguez
Chief
Facilities Management and Security Services

10.2.18
Physical Access Control (PAC)

Table of Contents

10.2.18.1
(07-05-2018)
Program Scope and Objectives

(1) This IRM section applies Physical Access Controls (PAC) to IRS facilities and space (work areas). PAC is 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
(02-03-2023)
Background

(1) PAC is 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 and out of the facility 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, Personnel Security, Contractor Investigations* provides policy and describes the background investigative requirements for contractor employees (and contractor personnel), 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
(07-05-2018)
Authority

(1) *Homeland Security Presidential Directive (HSPD)-12* - Policy for a Common Identification (ID) Standard for Federal Employees and Contractors

(2) *Department of Homeland Security (DHS) Interagency Security Committee (ISC) Standards*

(3) *Treasury Department Publication (TD P) 15-71, Security Manual*

(4) *Federal Information Processing Standards (FIPS) Publication 201*

(5) *OMB Memorandum M-05-24*: Implementation of Homeland Security Presidential Directive (HSPD) -12 - Policy for a Common ID Standard for Federal Employees and Contractors

10.2.18.1.3
(02-03-2023)
Responsibilities

(1) The Chief, FMSS prescribes and is responsible for oversight of PAC policy and guidance.

(2) FMSS AD, Security is responsible for oversight of the planning, developing, implementing, evaluating, and controlling PAC policy and guidance.

(3) FMSS AD, Operations and Territory Managers (TM) are responsible to ensure Security Section Chiefs (SSC) follow IRS policy and provide oversight in the implementation and enforcement of the PAC Program.

(4) FMSS SSCs are responsible for implementing and enforcing the PAC Program within their assigned territory, ensuring that IRS policy and procedures 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 security requirements.
b. Determining 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 security 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 "qualified escort."

(7) FMSS Headquarters 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
(02-03-2023)
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 procedures designed to admit only authorized personnel into IRS facilities.

(3) **Program Reports**: The authoritative data source for monitoring the PAC will be:

a. Access Control Records
b. Form 5421, *Limited Area Register (LAR)*
c. SAMC Incident Reports
d. Visitor Access Register (VAR)

(4) **Program Effectiveness**: PAC Program Review of 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. This IRM's formal review constitutes an evaluation of the programs' effectiveness.

(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
(02-03-2023)
Program Controls

(1) Analysis of the Facility Security Assessments (FSA) findings and recommendations.

10.2.18.1.6
(02-03-2023)
Terms and Acronyms

(1) **Access** - The authority granted to employees and contractors that provide 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, see IRM 10.23.1, *National Security Positions and Classified Information* and IRM 10.23.2, *Personnel Security, 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 and/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's Representative (COR)** - An individual designated and authorized by the contracting officer to perform contract administration activities on his/her behalf within the limits of delegated authority for a specific acquisition or contract.

Note: For additional information, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

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

Note: For additional information, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

(6) **Employee** - A federal employee, employed by the IRS.

(7) **Escorted Access** - A situation where a contractor employee not yet granted staff-like access that needs to be accompanied by a "qualified escort" during work performance and movement throughout the facility.
Extended definition: a situation where an individual (i.e., employee, contractor, visitor, or vendor) is not approved for staff-like access and requires escorted access.

Note: For additional information, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

(8) **Facility Access** - Controlled entry into a facility based on access status, role or function and employment category.

(9) **Limited Area** - An area to which access is limited to authorized personnel only and requires two-factor authentication mechanism to gain access.

Note: For additional information, see IRM 10.2.14, *Physical Security Program, Methods of Providing Protection*.

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

(11) **Perimeter Vehicle Access Register (PVAR)** - Daily record of vehicles, without passes, entering the perimeter.

(12) **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, see IRM 10.2.18.6.2, *Escorted Access*.

(13) **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, bi-monthly, or every four months).

(14) **Staff-like Access** - Authorized unescorted access to IRS-owned or controlled facilities, 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, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

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

Note: For additional information, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

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

Note: For additional information, see IRM 10.23.2, *Personnel Security, Contractor Investigations*.

(17) **Visitor** - A person visiting an IRS facility who has not been issued an IRS photo 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.

(18) **Visitor Access Register (VAR)** - Daily record of visitors entering the perimeter or the facility.

(19)

Acronyms

Acronym	Definition
AAL	Authorized Access List
AD	Associate Director
BB	Ball Bearing
BOD	Business Operating Division
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
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
FSL	Facility Security Level
HCO	Human Capital Office
HSPD	Homeland Security Presidential Directive
ICMIS	Identity Card Media Issuance System
ID	Identification
IG	Inspector General
ISC	Interagency Security Committee
IT	Information Technology
LAR	Limited Area Register
NTEU	National Treasury Employees Union

Acronym	Definition
NWDTP	National Weapons and Detection Program
OEP	Occupant Emergency Plan
PAC	Physical Access Control
PVAR	Perimeter Vehicle Access Register
POC	Point of Contact
PSO	Protective Security Officer
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
TD P	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
(02-03-2023)
Related Resources

(1) IRM 1.4.6, *Resource Guide for Manager, Managers Security Handbook*

(2) IRM 10.2.5, *Identification Media*

(3) IRM 10.2.8, *Incident Reporting*

(4) IRM 10.2.14, *Physical Security Program, Methods of Providing Protection*

(5) IRM 10.5, *Privacy and Information Protection*

(6) IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*

(7) IRM 10.23.1, *National Security Positions and Access to Classified Information*

(8) IRM 10.23.2, *Personnel Security, Contractor Investigations*

10.2.18.2
(07-05-2018)
Prohibited Items

(1) Unless in the lawful performance of official duties, 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, Code of Federal Regulations (CFR).* 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, includes Ball Bearing (BB) or pellet guns, compressed air guns, antique firearms, flare guns, knives or other devices with blades in excess of 2.5 inches, swords, explosives, incendiary devices, night sticks, brass-knuckles, throwing stars, pepper spray, (or any aerosol self-defense spray) etc.
c. Dangerous weapons.
d. Explosives.
e. 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 may be denied access if they attempt to enter a facility with prohibited items.

(3) In certain circumstances, the assigned FMSS Physical Security Staff may modify 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*.

10.2.18.3
(02-03-2023)
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) Alternative methods of screening personnel must be considered and implemented by the FMSS Physical Security Section Chief (SSC), with FMSS TM approval. 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 by someone of the same gender (preferred) if items not removed cannot be observed. As far as gender is considered, a Protective Security Officer (PSO) of the opposite gender may conduct a pat-down when a PSO of the same gender is not available. PSOs have special instructions on how to conduct opposite gender pat-downs.

c. Removal of all personal belongings from pockets/person for x-ray screening or visual inspection.
d. Some other optional and reasonable screening methodology, per local procedures.

(5) 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. For additional information, see subsection 10.2.18.15, *Deviations*.

10.2.18.4
(02-03-2023)
Random Occupant Screening Requirements

(1) Random Occupant Screening (ROS) are an integral part of physical security that contributes to IRS facilities' overall security posture.

(2) ROS of all personnel will be conducted:

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, and
d. In accordance with Federal Protective Service (FPS) policy and Interagency Security Committee (ISC) Standards.

(3) SSCs must coordinate with FPS to ensure that ROS is implemented and conducted in accordance with ISC Standards.

10.2.18.5
(02-03-2023)
Vehicle Screening Requirements

(1) Conduct vehicle screening in accordance with ISC Standards.

10.2.18.6
(02-03-2023)
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 subsection IRM 10.2.18.6, *Physical Access Eligibility Requirements*, *IRM 10.23.2, Personnel Security, Contractor Investigations* and *IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance* .

(3) A daily 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 issued Identification (ID) card.

Note: For additional information, see subsection 10.2.18.8.1, *Facility Unescorted Access*.

b. Escorted access.

(4) VAR is used at IRS facilities (owned or leased) where 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 Facility Security Committee (FSC) will make the VAR use determination, in consultation with the FSC IRS representative, and the security organization responsible for the facility.
b. At IRS facilities, where the lessor provides facility access control using guard PSO services, the assigned FMSS Physical Security Staff or designee will coordinate with the lessor to implement VAR requirements.
c. At IRS facilities dedicated solely to Taxpayer Assistance Centers (TAC) operations are exempt from VAR requirements.
d. FSL/VAR Matrix.

FSL	Condition	Procedure
III, IV, and V	IRS sole tenant and PSOs 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 PSOs	Assigned FMSS Physical Security Staff or designee coordinates with lessor to implement VAR
I and II	IRS sole tenant and control facility access (no PSOs)	VAR is not required
TAC	Locations or without PSO services	VAR is not required. Note: TAC taxpayer or visitor tracking, if required will be conducted as per TAC guidance and/or via 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 POC
b. Visitor name and contact information
c. Reason for visit
d. Rooms/Areas to be visited
e. Actual Date(s)/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, Personnel Security, Contractor Investigations*,
c. Documented completion of designated Security Awareness Training (SAT) as set forth in *IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance*, and
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, and
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, see *IRM 10.23.2, Personnel Security, 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 sponsoring the escorted individual(s) is responsible for providing qualified escort(s). Similarly, Business Unit managers are responsible for ensuring their designated escort(s) meet qualified escort requirements.

10.2.18.7
(02-03-2023)
Perimeter Access

(1) Perimeter access is controlled at locations where IRS is responsible for perimeter security and includes pedestrian and vehicular access.

(2) Employees and contractors that have an IRS issued photo ID card and 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 manned 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 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. Date of issue

(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
(02-03-2023)
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, during ROS or heightened security alerts, or when EPACS is not installed or inoperative, assigned PSOs must:

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, and
e. Visually check the card security feature(s).

(3) ID cards must be worn at or above the waist and visible from the front when in IRS facilities.

10.2.18.8.1
(02-03-2023)
Facility Unescorted Access

(1) Only employees, IRS contractors, other federal agency employees and contractors, that meet the eligibility requirements as outlined in subsection 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 ID 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 unauthorized persons to follow behind (also known as "tailgating" or "piggybacking") 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 subsection 10.2.18.6.2 (3), *Escorted Access*, for the requirements for qualified escort(s).

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

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

10.2.18.9.1
(02-03-2023)
Executive Service Employees

(1) The following Head of Office will be granted multi-facility or nation-wide facility access as required:

a. Commissioner of Internal Revenue Service
b. Deputy Commissioner, Services and Enforcement
c. Deputy Commissioner, Operations Support
d. Commissioner's Office & Chief of Staff
e. Commissioner, Large Business and International Division
f. Commissioner, Small Business/Self-Employed Division
g. Commissioner, Tax Exempt and Government Entities Division
h. Commissioner, Wage and Investment Division
i. Chief, Facilities Management & Security Services
j. Chief, IRS Independent Office of Appeals
k. Chief, Communications and Liaison

l. Chief, Criminal Investigation
m. Chief, Diversity Officer
n. Chief, Financial Officer
o. Chief, Human Capital Officer
p. Chief, Information Officer
q. National Taxpayer Advocate
r. Chief, Data and Analytics Officer
s. Chief, Privacy Officer
t. Director, Return Preparer Office
u. Director, Online Services
v. Director, Whistleblower Office
w. Chief, Risk Officer
x. Chief, Procurement Officer
y. Director, Office of Professional Responsibility
z. Chief, Taxpayer Experience Officer
aa. Principal Deputy Chief and Deputy Chief Counsel
ab. Assistant Deputy Commissioner for Operations Support
ac. Co-Directors, Enterprise Digitalization and Case Management
ad. Assistant Deputy Commissioner for Service and Enforcement
ae. *Senior Commissioner's Representative-Continuity of Operation (SCR-CO)

Note: *Territorial Access

10.2.18.9.2
(02-03-2023)
Non-Executive Service Employees/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 subsection 10.2.18.6,
b. Secure approval of the manager or COR, and
c. Access can be supported by EPACS.

(2) Employees or contractors must contact the assigned FMSS Physical Security Staff to ascertain the procedures for granting access to a facility that is not their assigned Post of Duty (POD).

(3) For facilities without EPACS that are utilizing key/lock, cipher lock (combination), or a legacy Identification Card Media Issuance System (ICMIS) for granting facility access, the employee or contractor must contact the assigned FMSS Physical Security Staff to ascertain procedures to issue keys, combination, or ICMIS card.

(4) A workspace reservation (hoteling) does not grant access to the building or IRS office space.

(5) Employee or contractor lists, or rosters are not authorized 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 two-factor authentication mechanism to gain access as described in *IRM 10.2.14, Physical Security Program, Methods of Providing Protection*. Access, unescorted or escorted, must be approved by the Business Unit 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
(02-03-2023)
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. Are approved by the Business Unit manager/supervisor responsible for the area,
c. Possessing a SmartID card with a "R" indicator, and
d. Placed on a designated AAL for the Limited Area.

Note: The Business Unit supervisor is a front-line manager that is delegated, by the Business Operating Division (BOD) or department-level manger, 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 LAR. However, identity verification and a signature will be required for issuance of a temporary access card to the Limited Area.

10.2.18.10.2
(02-03-2023)
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 SmartID card without an "R" indicator.

(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/manned Limited Area, a Limited Area Monitor (Business Unit staff) 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 an appropriate Limited Area ID card, upon verification of identity. If the visitor is an IRS employee not assigned to the area, an exchange of ID cards will be made,
d. Collect the ID card from visitors leaving the areas, and
e. Enter the time of the visitor's departure 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
(02-03-2023)
Limited Area Security and Administration

(1) Business Units 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 Limited Area manager. The Limited Area manager will review the register and retain it for at least one year. The managerial review is designed to ensure that only authorized individuals with an official need, have access to the Limited Areas.

(3) 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 Business Unit 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 Business Unit manager/supervisor responsible for the Limited Area must maintain the original AAL and LAR.
f. Only copies of the forms are authorized to be disseminated to those with an official need to know.

(4) Limited Area Monitors (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 his/her card and pin number (if required) to unlock the door every time he/she enters 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 without card readers.
b. Entrances without card readers. Authorized individuals must display their ID card to the monitor each time they enter the area.
c. Lost or forgotten ID cards. Use escorted access procedures until ID card is found or re-issued.
d. The monitor maintains an AAL for all personnel whose ID cards are not coded for the Limited Area, but who are authorized unescorted access to the Limited Area. Only the applicable Business Unit manager, or his/her designated representative, can add a name to this AAL and must be done in writing. Visits to the Limited Area by AAL personnel do not need to be recorded on the LAR.

(5) Limited Area Monitors (Receptionist) Requirements-Visitors. The Limited Area monitor will:

a. Process all visitors who need to enter the Limited Area per subsection 10.2.18.10.2,
b. Record visitors to the Limited Area on the Form 5421, *Limited Area Register*, and
c. Issue a Limited Area (Escort Only) access card as required.

10.2.18.11
(02-03-2023)
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 SmartID card at facility entry points. TIGTA employees entering IRS facilities without their SmartID card are subject to the escorted access requirements as outlined in subsection 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 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 on the facility public areas to discuss Union-business with individuals or small groups of employees who are members of the business unit. Such representatives must comply with all IRS security requirements and access to the facility.

10.2.18.14
(02-03-2023)
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 regulations to provide access to PAS personnel for individuals who need them because of certain disabilities.

Note: See 29 C.F.R.§ 1614.203(d)(5). PAS are services that help individuals who, because of targeted disabilities, require assistance to perform basic activities of daily living, like eating and using the restroom.

(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 subsection 10.2.18.6.1.
b. PAS escorted access will be consistent with subsection 10.2.18.6.2.

10.2.18.15
(02-03-2023)
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 Policy, for coordination and approval.

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*.