MANUAL TRANSMITTAL

10.2.1

Department of the Treasury
Internal Revenue Service

JANUARY 11, 2023

EFFECTIVE DATE

(01-11-2023)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.2.1, Physical Security.

MATERIAL CHANGES

(1) This IRM was updated to reflect current organizational titles, terminology, references, and citations.

(2) Integrated and updated requirements from the IRM 10.2.11, Basic Physical Security Concepts, and Interim Guidance Memoranda (IGM) policy documents:

a. IGM FMSS-10-0321-0001 Replacement of Security Information Management System (SIMS) with Security+ for IRM 10.2.11
b. IGM FMSS-10-0422-0004 Audit Management Checklist (AMC) and Corrective Actions Report (CAR)

(3) Integrated relevant portions of IRM 10.2.11 Basic Physical Security Concepts to allow for obsoletion.

(4) Replaced reference of Facility Security Assessment Addendum with Facility Security Compliance Assessment in paragraph 10.2.1.3.1.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 10.2.1 dated August 20, 2020.

AUDIENCE

Servicewide

Richard L. Rodriguez
Chief
Facilities Management and Security Services

10.2.1
Physical Security

Table of Contents

10.2.1.1
(01-11-2023)
Program Scope and Objectives

(1) **Purpose**: The purpose of this IRM is to establish the responsibilities for IRS Physical Security programs protecting IRS facilities, personnel, and assets.

(2) **Audience**: Servicewide.

(3) **Policy Owner**: Chief, FMSS.

(4) **Program Owner**: FMSS Associate Director (AD), Security.

(5) **Primary Stakeholders**: FMSS and Business Unit executives.

10.2.1.1.1
(01-11-2023)
Background

(1) To safeguard the security and safety of facilities, personnel, and assets, IRS develops and implements physical security policies, procedures, and processes to mitigate current and emerging risks.

10.2.1.1.2
(01-11-2023)
Authority

(1) Executive Order 12977, Interagency Security Committee

(2) Treasury Security Manual (TD P 15-71)

10.2.1.1.3
(01-11-2023)
Responsibilities

(1) Chief, FMSS:

a. Prescribes the IRS Physical Security Program through policy.
b. Provides oversight, guidance, and resources to ensure an effective IRS Physical Security Program.

(2) AD, Security:

a. Develops, implements, and evaluates IRS Physical Security Programs in accordance with federal regulations and laws, Department of Treasury Directives, and Interagency Security Committee (ISC) standards for the physical protection of facilities, personnel, and assets to ensure the continued operation and fulfilment of functions and services.
b. Maintains awareness of current and emerging security risks and industry-wide standards to support the analysis and selection of countermeasures.
c. Standardizes physical security equipment at IRS-controlled facilities.
d. Approves deviations of security policy.

(3) AD Operations and Territory Managers:

a. Oversee the IRS Physical Security Program in their assigned areas and territories.
b. Provide guidance, oversight, and assistance for the Physical Security Program.

(4) FMSS Security Section Chiefs (SSC):

a. Manage physical security programs within their territory, including planning, development, implementation, and evaluation.
b. Confirm that implementation of IRS physical security policy and procedures meets established minimum baseline level of protection requirements as per ISC and Department of Treasury guidance.

(5) IRS Employees and Contractors:

a. Comply with established physical security policies, practices, and procedures.

10.2.1.1.4
(01-11-2023)
Program Management and Review

(1) **Program Goals:**

a. Establish appropriate physical security measures, processes, and procedures to best protect IRS personnel, assets, and information.
b. Comply with federal regulations and laws, Treasury Directives and Department of Homeland Security (DHS) ISC standards.

(2) **Program Reports:**

a. Security+ reports.
b. Facility Security Compliance Assessments (FSCA).
c. Facility Security Plans (FSP).
d. Situational Awareness Management Center (SAMC) Incident Reports.

(3) **Program Effectiveness:**

a. Implementation of countermeasures, mitigation of vulnerabilities, or approved acceptance of risk for recommendations in Facility Security Assessment (FSA) and FSCA reports.
b. Compliance with ISC standards, as validated in the FSA reports. Compliance with Treasury and IRS requirements, as validated in the FSCA reports.
c. Completion of reporting requirements by suspense dates, as applicable.

10.2.1.1.5
(01-11-2023)
Program Controls

(1) **Annual Review:**

a. Review the processes included in this manual annually to ensure accuracy.

10.2.1.1.6
(01-11-2023)
Acronyms

(1)

Acronym	Definition
AD	Associate Director
AO	Administrative Officer
CI	Criminal Investigation
CR	Commissioner's Representative
DHS	Department of Homeland Security
EO	Executive Order
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
FSA	Facility Security Assessment
FSCA	Facility Security Compliance Assessment
FSL	Facility Security Level
FSP	Facility Security Plan
ISC	Interagency Security Committee

Acronym	Definition
OEP	Occupant Emergency Plan
PAC	Physical Access Control
PGLD	Privacy, Governmental Liaison, and Disclosure
SAMC	Situational Awareness Management Center
SBU	Sensitive But Unclassified
SSC	Security Section Chief
TDP	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration

10.2.1.1.7
(01-11-2023)
Related Resources

(1) *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, latest edition.*

(2) *IRM 1.4.60, Enterprise Risk Management Program.*

(3) *IRM 6.800.2, Employee Benefits, IRS Telework Program.*

(4) *IRM 10.2.8, Incident Reporting.*

(5) *IRM 10.2.18, Physical Access Control (PAC).*

(6) *IRM 10.5.1, Privacy and Information Protection, Privacy Policy.*

10.2.1.2
(01-11-2023)
Basic Physical Security Principles

(1) The main principles of physical security in the IRS:

a. Physical security programs are designed to mitigate risk, based on the ISC risk management process.
b. All managers and employees are integral to ensuring the physical security facilities, personnel, and assets.
c. Compliance with policies provides appropriate protection of IRS facilities, personnel, and assets.

10.2.1.3
(01-11-2023)
Interagency Security Committee (ISC)

(1) The ISC was established by Executive Order (EO) 12977 and collaboratively establishes policies, monitors compliance, and enhances the security and protection of Federal Facilities. The ISC, which consists of Federal departments and agencies, has a mandate to enhance the quality and effectiveness of physical security in, and the protection of, nonmilitary Federal facilities, and to provide a permanent body to address continuing governmentwide security issues for these facilities.

10.2.1.3.1
(01-11-2023)
Facility Security Assessments

(1) The IRS integrates two types of facility security assessments to serve as the official IRS risk assessment for each facility: the FSA and FSCA.

Note: The FSCA replaces the Facility Security Assessment Addendum used previously.

a. The Department of Homeland Security (DHS)/Federal Protective Service (FPS) regularly conducts the FSA to identify threats, vulnerabilities, and required countermeasures to mitigate risk, which serves as the foundation for the IRS FSCA.
b. While FPS utilizes the ISC standards for their assessment, FMSS Physical Security staff utilize IRS and Treasury-specific requirements to complete a FSCA at all locations where IRS employees are assigned.

(2) FPS will conduct an FSA at Child Care Centers, credit unions or parking lots within government facilities, but are not within IRS controlled perimeter and/or facility access. No IRS FSCA is required for these types of facilities and locations.

a. All FSA and FSCA risk assessment documents will be marked Sensitive but Unclassified (SBU) and handled in accordance with Treasury Directive Publication (TDP) 15-71.

(3) An FSA should be completed prior to personnel occupying new or leased facilities. However, if that is not possible, an FSA must be completed no later than six months after occupancy.

10.2.1.3.2
(01-11-2023)
Facility Security Plan (FSP)

(1) The FSP provides summary information used to describe significant safeguards and security programs at facilities occupied by IRS personnel. The FSP will be completed annually, by September 30th, for each IRS facility per ISC standards.

10.2.1.3.3
(01-11-2023)
Facility Security Committee (FSC)

(1) Every multi-tenant federal facility, either owned or leased, is required by the ISC to have a Facility Security Committee per **The Risk Management Process: An Interagency Security Committee Standard.** The FSC provides a standing body to address facility-specific security issues to ensure the protection of federal employees, essential functions, and government property.

(2) Physical security issues most often arise from the FSA. The FSC will address and vote to either implement the recommended countermeasure; mitigate the vulnerability; or accept risk.

(3) The assigned physical security staff will provide recommendations to the Tenant Representative for all required FSC votes.

a. When IRS is the lead tenant in a facility, the Commissioner's Representative (CR) or Administrative Officer (AO) will serve as the Designated Official and Chair the FSC.
b. When IRS is not the lead tenant; the CR or AO will serve as the Tenant Representative and is required to vote on physical security recommendations on behalf of IRS.

(4) Designated Officials and Tenant Representatives are required to successfully complete training, as noted in the ISC standard, prior to assuming duties on the FSC.

Note: For additional information on the FSC, see **The Risk Management Process: An Interagency Security Committee Standard**

(5) The FSC cannot impose, upgrade, downgrade, or remove countermeasures affecting IRS exclusive space.

10.2.1.4
(01-11-2023)
Risk Management

(1) The ISC established physical security standards and requirements for facilities based on the assigned Facility Security Level (FSL). When required countermeasures cannot be implemented due to facility structure, cost, or other issues, then risk management procedures must be followed per the *IRM 1.4.60, Enterprise Risk Management (ERM) Program.*

10.2.1.5
(01-11-2023)
IRS Telework Program

(1) The IRS Telework Program provides employees the opportunity to perform their duties at alternate worksites remote to the conventional office site (e.g., satellite locations, employee's residence). Employees are responsible for protecting all government records and data against unauthorized disclosure, access, mutilation, obliteration, or destruction. All managers must ensure employees are implementing the requirements in *IRM 6.800.2, Employee Benefits, IRS Telework Program* and *IRM 10.5.1, Privacy and Information Protection, Privacy Policy.*

10.2.1.6
(01-11-2023)
Off-Site Facilities

(1) Protection provided to off-site facilities, such as satellite buildings, and/or storage facilities, associated with Computing Centers and/or Campus locations, will depend on the usage of the space. The need for security guard services, security countermeasures, limited areas, and other types of security areas will be evaluated on an individual basis by the assigned physical security staff.

10.2.1.7
(01-11-2023)
Release of Security Information

(1) Territory Managers and Security Section Chiefs may authorize the release of security information (e.g., video surveillance images; visitor access records).

Acceptable requests for security information are requests:

a. From law enforcement officials, as part of an ongoing investigation.
b. Through an official subpoena request process found at Disclosure Knowledge Management.
c. From Criminal Investigation (CI), as part of an ongoing CI investigation.
d. From Treasury Inspector General for Tax Administration as part of an ongoing TIGTA investigations.
e. From Chief Counsel, General Legal Services pursuant to civil matters.
f. From FMSS Quality Assurance for audit purposes.
g. From Privacy, Governmental Liaison, and Disclosure (PGLD) staff.

Note: Requests received that do not meet the above acceptable criteria shall not be processed.

(2) All requests for security information must:

a. Be in writing.
b. Contain a legal justification.
c. Be validated with the requesting agency by approving officials prior to release.

(3) Business Units and managers are prohibited from utilizing security information (e.g., video surveillance images; visitor access records) for employee-related issues (e.g., entrance/exit of facilities).