MANUAL TRANSMITTAL

10.2.14

Department of the Treasury
Internal Revenue Service

JANUARY 10, 2023

EFFECTIVE DATE

(01-10-2023)

PURPOSE

(1) This transmits revised IRM 10.2.14, *Physical Security Program, Methods of Providing Protection*.

MATERIAL CHANGES

(1) This IRM was completely reorganized to reflect the Methods of Providing Protection to facilities, personnel, and assets, with updated terminology, links, and references.

(2) Integrated requirements from IRM 10.2.15, Minimum Protective Standards to allow for obsoletion and requires Business Units to determine what must be protected, while this IRM identifies the methods of providing protection.

(3) Incorporated and updated language from Facilities Management and Security Services (FMSS) *FMSS-10-0321-0001, Interim Guidance on replacement of Security Information Management System (SIMS) with Security+ for IRM 10.2.11 and IRM 10.2.14* into paragraphs 10.2.14.1.4 Program Management and Review and 10.2.14.2.2.2 Intrusion Detection Systems and Duress Alarms.

(4) Removed technical procedures throughout which are located within internal FMSS Standard Operating Procedures (SOP) and Scope of Work (SOW) documents.

(5) Updated definitions to avoid conflict with other IRM sections.

(6) Added new sub-sections Video Management, Receptacle and Container Placement, Heightened Security alerts, Mailroom/Mail Security, Workforce Security, Contract Security Services, and Security Reporting.

(7) Incorporated and updated language from Interim Guidance FMSS-10-0422-0005, Video Surveillance System (VSS) for IRM 10.2.14 into paragraph 10.2.14.2.3.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes 10.2.14 dated May 06, 2020.
This IRM Incorporates Interim Guidance FMSS-10-0422-0005, Interim guidance on Video Surveillance System (VSS) for (IRM 10.2.14), Methods of Providing Protection dated May 19, 2022.
This IRM Incorporates Interim Guidance FMSS-10-0321-0001, Interim Guidance on replacement of Security Information Management System (SIMS) with Security + for IRM 10.2.11, Basic Physical Security Concepts and IRM 10.2.14, Methods of Providing Protection dated February 22, 2021.

AUDIENCE

Servicewide

Richard L. Rodriguez
Chief
Facilities Management and Security Services

10.2.14
Methods of Providing Protection

Table of Contents

10.2.14.1 Program Scope and Objectives
10.2.14.1.1 Background
10.2.14.1.2 Authority
10.2.14.1.3 Responsibilities
10.2.14.1.4 Program Management and Review
10.2.14.1.5 Terms/Definitions/ Acronyms
10.2.14.1.6 Related Resources
10.2.14.2 Protecting Facilities and Personnel
10.2.14.2.1 Detection Systems
10.2.14.2.2 Intrusion Detection Systems and Duress Alarms
10.2.14.2.3 Video Surveillance Systems (VSS)
10.2.14.2.4 Video Management
10.2.14.2.5 Access Control
10.2.14.2.6 Locks
10.2.14.2.7 Security Section Chief (SSC) Key Control Responsibilities
10.2.14.2.8 Key Control Officer (KCO)
10.2.14.2.9 Key Control and Safeguarding
10.2.14.2.10 Enterprise Physical Access Control System (EPACS)
10.2.14.2.11 Separating Employee Clearance (SEC) - Accounting for Access Control Cards/Keys
10.2.14.2.12 Mail Security
10.2.14.2.13 X-ray Machines
10.2.14.2.14 Design for Blast Protection
10.2.14.2.15 Drop Boxes
10.2.14.2.16 Workforce Safety and Security
10.2.14.2.17 Receptacle and Container Placement
10.2.14.2.18 Heightened Security Alerts
10.2.14.3 Protecting Assets
10.2.14.3.1 Protected Items / Information
10.2.14.3.2 Normal Security
10.2.14.3.3 Locked Containers
10.2.14.3.4 Security Containers
10.2.14.3.5 Security Areas
10.2.14.3.6 Combination Control and Safeguarding
10.2.14.3.7 Clean Desk Policy
10.2.14.4 Contract Security Services

10.2.14.4.1 Protective Security Officers (PSO)
10.2.14.4.2 Explosive Detection Canine Program (EDCP)
10.2.14.5 Security Reporting
10.2.14.5.1 Security Hazards
10.2.14.5.2 Suspicious Activity/Items
10.2.14.6 Photography and Video Recordings Prohibition

10.2.14.1
(01-10-2023)
Program Scope and Objectives

(1) This section applies to the physical security countermeasures to be used for the protection of IRS facilities, personnel, and assets. Utilizing the principle of "security in depth," security begins at the outermost perimeter fence line, or entry into IRS space and inward to emplace and integrate security countermeasures. The IRS provides the baseline level of protection for all facilities, based on the current Facility Security Level (FSL) and in accordance with Interagency Security Committee (ISC) standards.

(2) **Purpose**: This IRM establishes the framework for applying physical security countermeasures to protect IRS facilities, personnel, and assets.

(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.

(7) **Program Goals**: To ensure the protection of IRS facilities, personnel, and assets through implementation of policies and procedures.

10.2.14.1.1
(01-10-2023)
Background

(1) To comply with Department of the Treasury, ISC, and IRS protection policies and standards, the IRS has established physical security methods of providing protection to protect IRS facilities, personnel, and assets.

10.2.14.1.2
(01-10-2023)
Authority

(1) General Services Administration (GSA) Facilities Standards for the Public Buildings Service (PBS) P100

(2) Treasury Department Publication (TDP) 15-71

(3) Executive Order (EO) 12977, Interagency Security Committee

(4) H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019

10.2.14.1.3
(01-10-2023)
Responsibilities

(1) The Chief, FMSS prescribes and oversees methods of providing protection policies and guidance.

(2) FMSS AD, Security:

a. Oversees planning, developing, evaluating, and controlling methods of providing protection policies and guidance.
b. Serves as approving authority for any deviation to existing security policies.

(3) Business Unit Managers must determine what assets and information within their unit require additional protection using the methods outlined in this policy and implement appropriate protection.

(4) FMSS Operations ADs and Territory Managers (TM) direct FMSS Security Section Chiefs (SSC) and oversee the implementation of this IRM.

(5) FMSS SSCs in each territory implement and enforce IRS policy and procedures for physical security issues within their assigned territory.

(6) All IRS managers:

a. Inform assigned employees of the importance adhering to facility security policies and practices.
b. Maintain awareness of physical security requirements within IRM 10.2.1 Physical Security Program series.
c. Purchase GSA-approved security containers required to support Business Unit needs ensure they are marked and maintained in accordance with requirements.
d. Initiate Personnel Actions Requests (PARs) and Separating Employee Clearance (SEC) actions in HRConnect.

Note: For additional information, see IRM 10.2.5, Identification Media.

(7) All employees and contractor employees must:

a. Comply with established security policies, practices, and procedures.
b. Report security hazards to assigned Physical Security staff, Protective Security Officers (PSO), or submit an *OS GetServices Knowledge Incident/Problem Service and Asset Management (KISAM)* request from the IRS Source homepage (Select New Ticket; Security Support; Physical Security; and select relevant reporting area).

Note: Physical Security staff coordinate security issues at each POD. Contact your Security Section Chief to identify the assigned person(s). Protective Security Officers are the uniformed security guards found at many IRS facilities.

10.2.14.1.4
(01-10-2023)
Program Management and Review

(1) **Program Reports:**

a. FMSS Security+ reports.
b. FMSS Facility Security Compliance Assessment (FSCA).

(2) **Program Effectiveness:**

a. Timely completion of Security+ reporting.
b. Analysis of countermeasures recommendations.

10.2.14.1.5
(01-10-2023)
Terms/Definitions/ Acronyms

(1) The following terms and acronyms are used throughout this IRM.

Term	Definition
Controlled Area	A security area which requires one single authentication mechanism to ensure only authorized personnel have unescorted access.
Countermeasure	Action, measure, or device intended to reduce an identified risk.

Limited Area	A security area to which access is limited to authorized personnel by a two-factor authentication mechanism.
Security Area	Consists of either controlled or limited areas, which require individual access authentication to gain entry.
Security Hazard	A situation which creates a vulnerability to protecting IRS facilities posed by an inoperable or ineffective security countermeasure.
Video Surveillance System (VSS)	VSS includes cameras, monitors, and video recorders to capture images in an area or around a building that transmitted over cabling to a recorder, so that the images can be viewed on a monitor in real time or later.

Acronym	**Definition**
AD	Associate Director
CI	Criminal Investigations
CNSI	Classified National Security Information
DHS	Department of Homeland Security
EO	Executive Order
EPACS	Enterprise Physical Access Control System
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
FSCA	Facility Security Compliance Assessment
GSA	General Services Administration
IDS	Intrusion Detection System
ISC	Interagency Security Committee
KCO	Key Control Officer
KCR	Key Custody Receipt
KISAM	Knowledge Incident/Problem Service and Asset Management

Acronym	Definition
PAC	Physical Access Control
PAR	Personnel Actions Request
PBS	Public Buildings Service
PSO	Protective Security Officer
SAMC	Situational Awareness Management Center
SEC	Separating Employee Clearance
SF	Standard Form
SSC	Security Section Chief
TDP	Treasury Department Publication
TIGTA	Treasury Inspector General for Tax Administration
TM	Territory Manager
VSS	Video Surveillance System

10.2.14.1.6
(01-10-2023)
Related Resources

(1) IRM 1.22.5, Mail Operations

(2) IRM 10.2.1, Physical Security

(3) IRM 10.2.5, Identification Media

(4) IRM 10.2.11, Basic Physical Security Concepts

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

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

(7) IRM 10.9.1, Classified National Security Information (CNSI)

10.2.14.2
(01-10-2023)
Protecting Facilities and Personnel

(1) The protection of facilities and personnel represents the highest IRS priority and includes most of our security programs.

(2) A facility's perimeter is usually identified by any type of barrier, and may include fences or gates, but will most often consist of the building wall.

(3) An important contributor to physical security is lighting used as a deterrent to detect intruders, illuminate areas to meet requirements for Video Surveillance System (VSS) coverage and assist response teams when responding to incidents at night.

10.2.14.2.1
(01-10-2023)
Detection Systems

(1) The use of specialized security equipment to detect security breaches is an essential component to providing security-in-depth for IRS facilities.

10.2.14.2.2
(01-10-2023)
Intrusion Detection Systems and Duress Alarms

(1) The IRS utilizes both Intrusion Detection Systems (IDS) and duress alarms in IRS facilities. These alarms are tested annually and when deemed necessary, by an FMSS alarm service vendor.

(2) IRS employees who work directly with taxpayers must familiarize themselves with the location and operation of duress alarms.

(3) Only assigned IRS FMSS Physical Security personnel or approved contractor employees are authorized to adjust, relocate, or remove security systems and alarms.

(4) All issues relating to IDS or duress alarms should be reported to the assigned physical security staff, or as noted below in 10.2.14.5.1 Security Hazards.

10.2.14.2.3
(01-10-2023)
Video Surveillance Systems (VSS)

(1) VSS is an essential IRS physical security countermeasure used for personnel protection, crime prevention and investigation. To support these efforts, position and direct VSS viewing fields to achieve the best possible coverage of IRS facility property. Facility or maintenance personnel must trim foliage that obstructs VSS fields of view.

(2) FMSS Physical Security determines IRS VSS requirements using security criterion from **The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B and IRS-FMSS Physical Security Design Manual.** VSS design will vary at each facility, based on its designated FSL and Physical Security Risk Assessment.

(3) Employee's personal workspace (e.g., office, cubicle) will not be viewed or recorded by VSS equipment.

(4) VSS data will not be used to verify employee attendance. Requests for all security recordings will be reviewed and approved or denied by the FMSS SSC or TM.

(5) VSS equipment operators are strictly prohibited from monitoring or tracking IRS personnel, contractors, or visitors without advance official authorization.

(6) VSS equipment used in IRS facilities must comply with the requirements outlined in H.R. 5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 and subsequent federal guidance. Contact the FMSS AD Security for a comprehensive list of prohibited telecommunications, VSS, equipment, and other items.

(7) In accordance with the *National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.6: Security Records Document 12829,* store video surveillance footage for 30 days. For storage requirements beyond 30 days submit justification via email to FMSS AD, Security.

10.2.14.2.4
(01-10-2023)
Video Management

(1) Video management software is authorized for use at IRS facilities, including, but not limited to the National Office, Enterprise Computing Centers, and campuses.

(2) FMSS AD Security must approve, in advance, video management software purchases and installations not previously approved and utilized by IRS.

10.2.14.2.5
(01-10-2023)
Access Control

(1) Effective safeguarding of IRS facilities, personnel and assets is reliant upon assuring that only authorized personnel, vehicles, and material are authorized for access and/or exit. Examples of access control include:

a. Key Locks - The potential for keys to be compromised by loss and making unauthorized duplicate keys should be considered when determining the security requirements. Examples of key locks include facility master keys, perimeter door keys, unissued limited area keys.
b. Combination and Cipher Locks - Utilized for padlocks, vaults, and doors. Combination and cipher-locks are easy to use but require additional handling and maintenance by the Business Unit. Examples of combination locks could include door cipher locks, security containers, safes, and vaults. Use combination locks sparingly and only within interior areas at facilities where access is essential at its perimeter.

Note: Electronic cipher locks may be utilized on FSL-1 exterior doors.

c. EPACS - EPACS grants or denies access with minimal delays and documents access.

10.2.14.2.6
(01-10-2023)
Locks

(1) The lock is the most accepted and widely used security device for protecting facilities, personnel, and assets.

(2) FMSS Security is responsible for managing facility master keys, perimeter door keys, and unissued limited area keys.

(3) Each Business Unit will manage their own office and storage keys, as well as combinations for door cipher locks, security containers, safes, and vaults.

(4) Business Unit managers will annually conduct an annual internal key inventory of all office keys within the Business Unit. Assigned FMSS Physical Security Staff are available to provide support, as necessary by the end of each fiscal year.

(5) Use Form 1930-D, Key Control Receipt (KCR) to issue all facility access and security area door keys. Complete the KCR, obtain all required signatures and the issuing authority (FMSS or Business Unit Manager) will maintain this record until the issued key is returned.

(6) Security area access door lock keys must be:

a. Labeled with an identifier unrelated to the room number
b. Engraved with the words **U.S. Government - DO NOT DUPLICATE.**

(7) Store security area keys not in personal custody of an authorized IRS employee in a GSA approved security container.

(8) Keep security area key and combinations issuance to the absolute minimum. Issue keys and combinations only to those individuals, preferably supervisors, who require after-hours access to the area.

10.2.14.2.7
(01-10-2023)
Security Section Chief (SSC) Key Control Responsibilities

(1) The SSC implements key control program policy requirements and guidelines by doing the following:

a. Designate a territory Key Control Officer (KCO), in writing.
b. Approve duplicate/additional keys for perimeter doors, limited/controlled area doors, and master key requests.

c. Review and certify the territory Key Control Registry (KCR) every fiscal year.
d. Assign a member of the Physical Security staff to identify key and lock requirements for territory space projects.

10.2.14.2.8
(01-10-2023)
Key Control Officer (KCO)

(1) The FMSS KCO will:

a. Review and certify territory KCR every fiscal year, to confirm all perimeter, master, and/or limited/controlled area keys are listed on the KCR for each territory facility.
b. Manage mechanical metal keys issuance, return and destruction for facility perimeter, limited/controlled areas, and master keys.
c. Secure FMSS-managed unused locks and padlock cores for assigned facilities in an approved security container.
d. Inform FMSS SSC of significant key/lock concerns (multiple missing keys, unrecoverable master key, chronic malfunctioning locks, etc.).
e. Within 10 business days, initiate the process to have the relevant locks re-keyed (new core installed) if a Business Unit Annual Key Inventory identifies more than a 5% loss of perimeter and or limited/controlled area keys.

10.2.14.2.9
(01-10-2023)
Key Control and Safeguarding

(1) The assigned FMSS SSC or designee must approve duplicate/additional key requests for perimeter doors, security area doors and security containers.

(2) FMSS Physical Security staff maintains all master keys (a key that can open all applicable IRS space with the exception of Criminal Investigations (CI) space) in a central location. Properly identify master keys to their corresponding doors (s). Exceptions may exist where the area is required to be "off-master."

Note: Criminal Investigation funds, controls, and maintains all keys to CI space.

(3) Limit key issuance to persons requiring access to an area, room , or container. Keep on-hand and keys issued to a minimum. A **"Master Key"** is issued to a limited number of personnel selected by the facility's issuing authority. Master keys will typically not be issued to more than 5% of an office population except when there are a small number of IRS employees in a post of duty. Individuals with an issued key must keep it in their possession and not duplicate it, leave it unsecured or loan it to another individual.

(4) FMSS Physical Security staff maintains extra locks and padlock cores supplies. FMSS provides two keys for each container (lateral) and padlock (upright with bar lock) to maintain security container (lateral and upright) integrity. If the central core of a security container lock or padlock is replaced with a non-security lock core, or has more than two keys, it is not considered secured.

10.2.14.2.10
(01-10-2023)
Enterprise Physical Access Control System (EPACS)

(1) EPACS is the IRS backbone for physical access and was established in response to Homeland Security Presidential Directive-12 (HSPD-12). EPACS allows or prevents access of personnel to a building, a room or security area quickly and effectively while minimizing risk.

(2) EPACS is the primary technical solution for electronic physical access control in the IRS. Where feasible, access to IRS facilities or space will be managed by installing EPACS in accordance with applicable current standards.

(3) The FMSS SSC will determine where EPACS is installed based on space configuration, type of existing hardware, type of partition walls, security risk assessment results, and ISC Standards. Submit requests for policy deviations by email via FMSS AD Operations to FMSS AD Security for review.

(4) Per Treasury Security Manual (TDP 15-71), "Access control systems shall provide auditable records of access."

Note: For additional information see IRM 10.2.18, Physical Access Control.

10.2.14.2.11
(01-10-2023)
Separating Employee Clearance (SEC) - Accounting for Access Control Cards/Keys

(1) Business Unit managers must use the automated HRConnect SEC Module to certify facility access door key return/recovery from separating employees.

(2) Business Unit managers must:

a. Complete PAR actions in HR Connect for separating employees.
b. Verify issued facility access door key(s) recovery from separating employees.
c. Report unrecovered facility access, limited/controlled area doors, and master keys to:

1. Situational Awareness Management Center (SAMC).
2. Treasury Inspector General for Tax Administration (TIGTA).
3. Assigned FMSS Physical Security staff.

(3) FMSS Physical Security staff routinely accesses the HRConnect SEC module to:

a. Check for any separating employee's access control cards and /or mechanical keys return/recovery
b. Document access card/mechanical key return/recovery in HRConnect SEC module.

Note: For additional information on the recovery of ID media, see IRM 10.2.5, Identification Media.

10.2.14.2.12
(01-10-2023)
Mail Security

(1) The IRS has four types of mailrooms per IRM 1.22.5, Mail Operations:

a. Submission Processing/Campus Mailrooms. Staffed by IRS employees and provides services to multiple locations.
b. Contract Mailrooms: staffed by contractor employees in field offices of more than 250 employees.
c. Shared Mailrooms: found in smaller Posts of Duty (POD) with 20-250 employees. Staffing is a shared responsibility by building occupants.
d. POD Mailrooms: PODs with less than 20 employees generally do not have an enclosed mailroom, but a location in the POD where incoming mail is sorted for employees.

Note: Submission Processing/Campus Mailrooms and Contract Mailrooms are designated as Limited Areas.

(2) While the threat of attack through the mail is rated low by the ISC, the IRS remains vulnerable to Chemical, Biological, or Radiological (CBR) dispersal and explosive devices transmitted through mail or delivery services.

(3) All designated mailrooms and mail opening areas must have Safe/Suspicious Mail Handling and Incident Reporting procedures posted for all mail opening employees and/or contractor employees to view. At a minimum, the following guidance and procedures will be posted within the mail area and employees when handling suspicious mail and packages.

(4) Features of a suspicious package or packages:

a. Has soft spots or is lopsided.
b. Wrapped with string.
c. Contains distorted handwriting.
d. Has leaks, stains, powders, or protruding materials.
e. Contains no or excess postage.
f. Contains an odor.

(5) Procedures to follow when handling suspicious letters and packages:

a. Remain calm.
b. Do not open the letter or package.
c. Do not shake or empty contents of package.
d. Do not carry the package to show it to others.
e. Make a list of all persons who touched the package.
f. Put the package on a stable surface.
g. Do not touch your eyes, nose, or other body parts.
h. Isolate the package and secure the room.
i. Wash your hands with soap and water.

(6) Reporting the incident:

a. Call first responders for your respective office (local guard service).
b. Report to your manager and call 911.
c. Contact Federal Protective Service (FPS) at 1-877-4FPS-411.
d. Contact TIGTA at 1-800-589-3718.
e. Report to SAMC within 30 minutes of incident discovery or as soon as safely possible.

(7) Incidents may be reported per IRM 10.2.8, Incident Reporting, to SAMC through any of the following methods:

a. Website: *https://tscc.enterprise.irs.gov/irc/*
b. Telephone: 1-866-216-4809
c. E-mail: *samc@irs.gov*

10.2.14.2.13
(01-10-2023)
X-ray Machines

(1) X-ray machines and metal detectors are utilized to scan for suspicious or prohibited items in packages, mail, or carried on a person. PSOs assigned to IRS facilities are specifically trained and tasked to screen and identify suspicious objects

(2) For FSL III - V facilities:

a. X-ray and metal detectors must be used by PSOs to screen all visitors and all occupants and their property that do not possess an acceptable ID for access to IRS space.

b. PSOs must screen all mail and packages using X-ray machines. Further requirements regarding location of the x-ray machine are based on facility layout and FSL and detailed in **ISC Risk Management Process for Federal Facilities, Appendix B: Countermeasures.**
c. PSOs must physically inspect items that cannot be passed through screening equipment.

10.2.14.2.14
(01-10-2023)
Design for Blast Protection

(1) Due to the danger of explosives being shipped and detonated during mail handling, the ISC identifies security criterion based on the FSL of the facility. Refer to **ISC Risk Management Process for Federal Facilities Appendix B: Countermeasures.**

10.2.14.2.15
(01-10-2023)
Drop Boxes

(1) Drop boxes, or any container used for the purpose of collecting items such as payments, mail, or information without human-to-human interaction are strictly prohibited.

10.2.14.2.16
(01-10-2023)
Workforce Safety and Security

(1) Facility Occupant Emergency Planning-The Occupant Emergency Plan (OEP) is the guide to ensure the IRS workforce is prepared and trained to respond to emergencies within each facility. See IRM 10.2.9, Occupant Emergency Planning for more information.

(2) Workplace Violence-FMSS authored the *Desk Guide for Workplace Violence Prevention and Response* to assist managers and employees; there are four categories of workplace violence.

a. Criminal Intent: The perpetrator has no legitimate relationship to the agency or its employees and is usually committing a separate crime, such as robbery, in conjunction with the violence.
b. Customer/Client: The perpetrator has a legitimate relationship with the agency and becomes violent while being served by the agency. This category includes customers, clients, and any other group for which the agency provides services.
c. Employee-on-Employee: The perpetrator is a current or former agency employee who attacks or threatens another current or former employee(s) in the workplace.
d. Personal Relationship: The perpetrator usually does not have a relationship with the agency but has a personal relationship with an agency employee, contractor, or customer.

(3) Domestic Violence, Sexual Assault, and Stalking. Human Capital Office (HCO) has centralized support information on the *Domestic Violence, Sexual Assault, and Stalking* website.

(4) Employee Protection, Privacy, Governmental Liaison, and Disclosure (PGLD) oversees two programs to identify taxpayers who represent a potential danger to employees: Caution Upon Contact (CAU) and Potentially Dangerous Taxpayer (PDT). IRS employees who have duties requiring taxpayer contact should be aware of both programs and can find information on the *Office of Employee Protection (OEP) website*.

10.2.14.2.17
(01-10-2023)
Receptacle and Container Placement

(1) Trash containers, mailboxes, donation/recycle containers, vending machines, and other similar objects must be positioned a minimum of 25 feet from building exterior and entry/exit points or implement blast containment measures to mitigate an explosion.

10.2.14.2.18
(01-10-2023)
Heightened Security Alerts

(1) ISC App B Countermeasures references "Heightened Security Alerts" and provides options relating to countermeasures based on the FSL. When localized risk increases, and upon notification of FPS, local law enforcement, or other federal agencies, SSCs must coordinate with FPS to review and implement the below, or other, recommended countermeasures.

a. Vehicle Screening: Screen visitor vehicles before entry into the controlled parking area. Randomly screen employee and contractor vehicles during heightened security alerts. (FSL IV-V)
b. Vehicle Access Points: Reducing the number of vehicle access points, particularly under periods of heightened security alerts, reduces vulnerability and security costs associated with monitoring and controlling access to the site. (FSL III-V)
c. Receptacle & Container Placement: When containers are used, ensure that they can be removed during periods of heightened security alerts. (FSL II-V)
d. Occupant Screening: During a heightened security alert, the FSC or tenant representative for single-tenant facilities should consider screening all "continuous" occupants. (All)
e. Limited Building Entry Points: Reducing the number of building entry points, particularly under periods of heightened security alerts, reduces vulnerability and security costs associated with monitoring and controlling access. (FSL III-V)

10.2.14.3
(01-10-2023)
Protecting Assets

(1) The basic principle of security within the IRS is to provide access to assets, including information, to persons with an established IRS business need.

10.2.14.3.1
(01-10-2023)
Protected Items / Information

(1) At least annually, each business unit must determine what items and information require protection beyond that of being in secure IRS space and establish internal procedures and controls to safeguard required items. There are four types of protection for consideration:

a. Normal Security
b. Locked Containers
c. Security Containers
d. Security Areas

10.2.14.3.2
(01-10-2023)
Normal Security

(1) Normal Security is the IRS standard and is appropriate for the majority of protected items. IRS space is designated as a controlled area and all visitors and contractor employees must be escorted unless they have been granted staff-like access by HCO Personnel Security. Additionally, the IRS has adopted general clean desk and containment objectives for the protection of taxpayer, privacy act, and other protected data.

Note: For additional guidance regarding clean desk policy and clean desk waivers, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy.

10.2.14.3.3
(01-10-2023)
Locked Containers

(1) For some items, such as Sensitive But Unclassified (SBU), Controlled Unclassified Information (CUI), or Identifiable Information, a standard locked container is sufficient. For additional information see IRM 10.5.1, Privacy and Information Protection, Privacy Policy.

(2) Locked containers are any lockable metal container with riveted or welded seams. All key and combination locks must be controlled by the business unit with oversight of the area with the same level of protection for the items being protected.

10.2.14.3.4
(01-10-2023)
Security Containers

(1) A security container will be used for storing items which Business Units or applicable federal regulations determine require a higher level of security, IRS utilizes either GSA-approved Class 5 or 6 security containers. All security containers must be marked on the outside of the front face of the containers "GSA Approved Security Container" and must be purchased through *GSA Global Supply*.

(2) Class 5 security containers have several types,

a. Filing Cabinets (Two or Four Drawer)
b. Map and Plan Container
c. Information Processing Systems (IPS) Container
d. Weapons Containers

(3) Class 6 security containers are specifically approved for storage of CNSI and must be equipped with a Federal Specification FF-L2740B compliant combination lock.

Note: For additional information regarding the storage of CNSI, refer to IRM 10.9.1 Classified national Security Information (CNSI).

(4) Containers in need of repair must be serviced by GSA certified technician to maintain the certification of the container.

(5) All combinations must be controlled by the Business Unit owning the security container.

10.2.14.3.5
(01-10-2023)
Security Areas

(1) The IRS has numerous areas which require additional protection due to the importance of their function or sensitivity of the information or assets. The degree of security and access control these areas require depends on the nature, sensitivity, and / or importance of the information and assets safeguarded. Examples include:

a. Large amounts of currency.
b. Mail processing centers.
c. Law enforcement investigative information.
d. Backup information systems.

(2) The IRS utilizes two types of security areas to restrict access: controlled and limited areas.

a. A Controlled Area requires a single-factor authentication mechanism. Each IRS Space is controlled area, which ensures only authorized personnel and visitors are allowed access. Additional controlled areas, which are considered "above standard" may be established within IRS

spaces for alarm panel rooms; security operations centers; rooms with large amounts of currency; or other similar areas within a business unit.

b. A Limited Area is an area to which access is limited to authorized personnel only and requires two-factor authentication mechanism. All personnel who access a Limited Area must have a verified official business need to enter.

(3) Managers may request their territory SSC to determine if additional levels of access control may be beneficial.

Note: The IRS Computer Rooms (Martinsburg, Memphis, Kansas City, Fresno, Austin, Ogden, and Detroit) are designated Limited Areas. Other IT assets such as IDF, MDF, CDF are designated as Controlled Areas and may be safeguarded with single -authentication access control (e.g., EPACS [preferred method where feasible], mechanical, or cipher locks) at the discretion of the owning business unit and concurrence of the Territory Section Security Chief (SSC) or servicing Physical Security staff.

10.2.14.3.6
(01-10-2023)
Combination Control and Safeguarding

(1) Each Business Unit manages combinations for their door cipher locks, security containers, safes, and vaults.

(2) Three-digit combinations are ten-times more susceptible to compromise than four-digit combinations. Door cipher locks must be programmed to a minimum four-digit combination.

(3) In accordance with Treasure Security Manual (TDP 15-71), the combination lock must be changed under any of the following conditions:

a. When the safe or lock is first placed into service.
b. When a person knowing the combination no longer requires access to it and other controls do not exist to prevent their access to the lock.
c. When a combination has been subjected to possible compromise, actual compromise, or unauthorized disclosure.
d. At least every three years unless conditions dictate sooner.

(4) Use OS GetServices KISAM to request all combination changes. Limit combination issuance to those with a need to access the area, room , or container. Maintain security container combinations by using Standard Form (SF) 700, Security Container Information (the form has three parts).

a. SF-700 Instructions

1. Complete Part I entirely (SF 700 input fields are self-explanatory).
2. Separate Part I and attach it to the inside container front control drawer (with the lock mechanism).
3. Record the combination on Part II.
4. Place Part II inside Part III and seal it.

Note: For additional guidance concerning the use of SF-700 for CNSI, see IRM 10.9.1, Classified National Security Information.

(5) Maintain safe and vault combination records (Parts II & III of SF-700) centrally within the local Business Unit management office.

(6) Place all completed SF-700 forms in a container with the same or higher security classification as the highest classified material stored in the container, or security area.

10.2.14.3.7
(01-10-2023)
Clean Desk Policy

(1) The IRS has adopted general clean desk and containment objectives for the protection of taxpayer, privacy act, and other protected data. There are certain areas, such as mass processing operations, where the full implementation of clean desk and/or containerization procedures are not appropriate.

Note: For additional guidance regarding clean desk policy and clean desk waivers, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy.

10.2.14.4
(01-10-2023)
Contract Security Services

(1) FMSS utilizes contractor support for the security functions of armed guards, explosive detection, credentialing, and countermeasures maintenance and testing.

(2) Any requests for changes or additional services must be initiated through the assigned Physical Security staff.

10.2.14.4.1
(01-10-2023)
Protective Security Officers (PSO)

(1) Guard services are provided for IRS facilities by the Department of Homeland Security (DHS)/FPS. DHS/FPS is solely responsible for the management and oversight.

(2) Any incidents or concerns relating to the performance of PSOs must be reported through SAMC and assigned Physical Security staff.

10.2.14.4.2
(01-10-2023)
Explosive Detection Canine Program (EDCP)

(1) Explosive Detection Canine Teams (EDCT) provide support to IRS facilities based on identified risks. EDCT consists of a dog and handler and are utilized to inspect all incoming mail, packages and other deliveries being made to IRS facilities prior to delivery and receipt by IRS personnel.

(2) EDCTs also conduct roving patrols, random security inspections, and provide emergency response to security incidents. EDCTs may utilized to support OEPs, Continuity of Operations, and law enforcement partners (e.g., n (CI), TIGTA, federal or local law enforcement), upon request.

10.2.14.5
(01-10-2023)
Security Reporting

(1) All IRS employees and contractor employees have a responsibility to report suspicious activity and hazards which impact the security of facilities, personnel, and assets.

10.2.14.5.1
(01-10-2023)
Security Hazards

(1) IRS facilities are protected with various security systems and equipment to deter and detect security breaches. To maintain an effective security posture, it is vital that security hazards are reported and monitored to resolution. Example of security hazards include

a. Lighting outages impacting video surveillance or personal observation.
b. Overgrown or downed trees, foliage, or other visual obstructions.
c. Inoperable cameras, alarm activation points, duress alarms, and intrusion detection systems.
d. Breaches (gaps, holes, etc.) in perimeter fencing.
e. Malfunctioning door locks or other access control issues.

(2) Most security hazards are identified by FPS personnel, PSOs during security patrols but reports from IRS personnel are encouraged and not uncommon.

(3) IRS personnel must report issues directly to PSOs, to assigned Physical Security staff, or open an OS GetServices KISAM " new ticket" request. Then, select " Order from Catalog; "Security Support," then Physical Security" and follow the links to describe the issue.

(4) Assigned Physical Security staff will:

a. Confirm with assigned FPS officers(s) that post orders for PSOs include the requirement that:

1. All identified security hazards are reported as soon as possible.
2. Security measures are implemented to mitigate risks until security hazard is resolved.

a. Track all *OS GetServices KISAM tickets* from submission to satisfactory completion

10.2.14.5.2
(01-10-2023)
Suspicious Activity/Items

(1) All suspicious activity or items must be reported immediately to assigned PSOs or Physical Security staff or through a SAMC report submission. Examples of suspicious activity or items include unattended boxes, packages, or bags in or near IRS or federal facilities; unmanned aerial systems/drones near or over IRS facilities; and potential surveillance of IRS facilities or personnel. For additional information, see IRM 10.2.8, Incident Reporting.

10.2.14.6
(01-10-2023)
Photography and Video Recordings Prohibition

(1) Photography within or on the grounds of IRS facilities and campuses is prohibited except when specifically authorized by the FMSS Physical Security Section Chief. Taking photographs of external features of a facility or other property which provides information not publicly accessible must be immediately reported to local FMSS Physical Security staff, the Treasury Inspector General for Tax Administration (TIGTA), and FPS. Photography is defined as the recording of images through physical or electronic means which include still photographs, x-ray images, and video.