EFFECTIVE DATE

(03-11-2024)

PURPOSE

(1) This transmittal revises IRM 10.2.5, Identification Media.

MATERIAL CHANGES

(1) This IRM was updated to reflect current organizational titles, scope, definitions, responsibilities, and authorized use.

(2) IRM 10.2.5.1.2, Authority: Added Delegation Order 1-51, Authority to Prescribe Identification.

(3) IRM 10.2.5.1.3, Responsibilities: Removed TIGTA reference due to policy change.

(4) IRM 10.2.5.1.4, Program Management and Review: added HRConnect Personal Identity Verification (PIV) Data Synchronization.

(5) IRM 10.2.5.1.6, Terms/Definitions/Acronyms: Subsection was formerly 10.2.5.1.5; addition of a subsection above resulted in its renumbering. Added definitions for alpha files, lost ID Card, compromised ID, proxy/access card, ID card and removed vehicle ID media and insignia.

(6) IRM 10.2.5.1.7, Related Sources: Subsection was formerly 10.2.5.1.6; addition of a subsection above resulted in its renumbering. Removed Form 13716 ID Media Request for Employees and Form 13716-A, Request for ID Media for IRS Non-Employees references due to form being obsolete.

(7) IRM 10.2.5.5, Authorized ID Media: Removed parking permits and insignia because this is out of the scope of ICAM.

(8) IRM 10.2.5.6, Photo ID Cards: Subsection was formerly 10.2.5.6.1; deletion of a subsection above resulted in its renumbering. Added self-expiring Visitor Management System (VMS) cards.

(9) IRM 10.2.5.6.1, Replacement ID Cards: Subsection was formerly 10.2.5.6.2; deletion of a subsection above resulted in its renumbering. Removed Form 13716 references, included proxy cards access to be revoked within 18 hours, and removed TIGTA reference due to policy change.

(10) IRM 10.2.5.6.2, Non-Photo ID cards: Subsection was formerly 10.2.5.6.3; deletion of a subsection above resulted in its renumbering. Removed Limited Temporary ID card references because these cards will no longer be issued. Added link to locate procedures for Limited Area Monitors.

(11) IRM 10.2.5.6.3, Proxy/Access Cards: Subsection was formerly 10.2.5.6.4; deletion of a subsection above resulted in its renumbering. Removed Form 13716, ID Media Request for Employees and Form 13716-A, Request for ID Media for Non-IRS Employees references because form is obsolete and added 10.2.18 reference.

(12) IRM 10.2.5.7, Recovery of ID Media: Subsection was formerly 10.2.5.9; deletion of a subsection above resulted in its renumbering. Removed TIGTA references due to policy change.

(13) IRM 10.2.5.8, Records and Accountability: Subsection was formerly 10.2.5.10; deletion of a subsection above resulted in its renumbering. Removed Form 13716, ID Media Request for Employees and Form 13716-A, Request for ID Media for Non-IRS Employees, updated document retention requirements and verification of card termination and destruction, and removed TIGTA references.

(14) Deleted subsection titled ID Cards, formally IRM 10.2.5.6, ID card definition was added to IRM 10.2.5.1.6, Terms/Definitions/Acronyms.

(15) Deleted subsection titled Vehicle ID Media, formally IRM 10.2.5.7, because the program is outside of the scope of ICAM.

(16) Deleted subsection titled Insignia, formally IRM 10.2.5.8, because the program is outside of the scope of ICAM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.2.5 dated April 28, 2021.

AUDIENCE

All IRS Organizations

Richard L. Rodriguez
Chief
Facilities Management and Security Services (FMSS)

10.2.5
Identification Media

Table of Contents

10.2.5.1
(04-28-2021)
Program Scope and Objectives

(1) This section applies to the control, issuance, and disposition of Identification (ID) media. ID media are authorized forms of ID that are designed to provide evidence of the bearer's identity, authorization to access IRS facilities or systems, or authority to act as an agent of the IRS in the performance of official duties.

(2) **Purpose**: This IRM provides an overview of the authorized forms of ID media issued by the IRS to employees and contractor employees, and establishes the policies for the control, issuance, and recovery of ID media.

(3) **Audience**: All IRS Organizations.

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

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

(6) **Primary Stakeholders**: FMSS, Field Operations.

(7) **Program Goals**: To affirm ID media is authorized for use by the IRS and establish the processes and procedures for the issuance, maintenance, and recovery of ID media to mitigate unauthorized access to IRS systems and facilities, and to protect IRS personnel, assets, and information.

10.2.5.1.1
(04-28-2021)
Background

(1) IRS ID media is issued solely for use by authorized IRS employees and contractor employees, other Federal agency employees and contractors, in the performance of official duties, and visitors (official or unofficial).

10.2.5.1.2
(03-11-2024)
Authority

(1) *Office of Management and Budget (OMB) M-05-24*: Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors

(2) *Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*

(3) *18 United States Code (USC) 499: Military, naval, or official passes*

(4) *18 USC 701: Official badges, identification cards, other insignia*

(5) *HSPD-12 - Policy for a Common Identification Standard for Federal Employees and Contractors*

(6) *Delegation Order 1-51, Authority to Prescribe Identification Media*

10.2.5.1.3
(03-11-2024)
Responsibilities

(1) The Chief, FMSS, is authorized to prescribe ID media for use within the IRS per Delegation Order 1-51, Authority to Prescribe Identification Media, located in IRM 1.2.2, Servicewide Policies and Authorities, Servicewide Delegations of Authority.

(2) The AD, Security, is responsible for oversight of ID media for use within the IRS.

(3) The Chief, Access & Identification Management (AIM), is responsible for oversight of the planning, developing, implementing, evaluating, and controlling the ID Media Program.

(4) The Chief, Identity Credential and Access Management (ICAM), is responsible for planning, developing, implementing, evaluating, and controlling the ID Media Program.

(5) FMSS Territory Managers (TM) are responsible for ensuring FMSS Security Section Chief(s) (SSC) follow IRS policy and provide oversight in the implementation and enforcement of the ID Media Program.

(6) FMSS SSC are responsible for implementing and enforcing the ID Media Program within their assigned territory, ensuring that IRS policy and procedures are followed.

(7) All IRS managers, Contracting Officer's Representatives (COR), and Government Officials with personnel administrative functions have a responsibility for:

a. Informing all employees in their span of control of the importance of following ID media practices.
b. Verifying only authorized employees and contractor employees are in the work area for which they are responsible.
c. Immediately challenging and reporting the presence of suspected unauthorized persons in a work area to their local security office.
d. Ensuring that authorized employees in their span of control are issued the appropriate ID media, use, and display their ID media in accordance with the requirements of this IRM.
e. Recovering ID media of employees and contractor employees who separate or are placed in non-work status on their last workday and immediately sending the recovered ID media to the local FMSS security office for disposition or retention.
f. Reporting unrecovered ID media of employees and contractor employees who separate or are placed in non-work status to the local FMSS security office and the Situational Awareness Management Center (SAMC) in accordance with IRM 10.2.8, Incident Reporting.
g. Certifying the disposition of issued ID media items to include the return of recovered ID media items to the local FMSS security office, using the automated Human Resources (HR) Connect Separating Employee Clearance (SEC) module for employees, and attaching Form 14604, Contractor Separation Checklist, to the Separating Contractor Clearance (SCC) module for contractor employees.
h. Completing a request for a replacement ID media for their employees and contractor employees by scheduling an appointment at a local credentialing office.
i. Ensuring staff-like access eligibility requirements are met, as per IRM 10.2.18, Physical Access Control.
j. Ensuring all contractor employees in their span of control complete Security Awareness Training (SAT) timely in accordance with IRM 10.23.2, Personnel Security, Contractor Investigations, and ensuring it is documented in Integrated Talent Management (ITM).

(8) All personnel issued ID media are responsible for:

a. Safeguarding their ID media.
b. Displaying their ID media in accordance with this IRM while in IRS facilities or performing work duties.
c. Presenting their ID card when requested by their manager, the COR, or the local FMSS security office to allow for IRS accountability of ID media.

d. Returning their ID media to their manager or COR or Government Official with personnel administrative functions when placed in a non-work status or upon separation from the IRS.
e. Promptly reporting lost or stolen ID media to their manager or COR, the local FMSS security office, and to SAMC in accordance with IRM 10.2.8, Incident Reporting.

10.2.5.1.4
(03-11-2024)
Program Management and Review

(1) **Program Reports**:

a. HRConnect Personal Identity Verification (PIV) Data Synchronization
b. USAccess Applicant Status Report

(2) **Program Effectiveness**:

a. Timely revocation of physical access
b. Recovery of all ID media from unauthorized persons
c. Timely completion of all SmartID card maintenance requirements
d. Issuance of ID media only to authorized employees and contractor employees

10.2.5.1.5
(03-11-2024)
Program Controls

(1) **Annual Review**: ICAM conducts annual reviews to assess all processes of the program and ensures the program operates in compliance with laws and regulations of the Department of the Treasury ("Treasury").

(2) Track ID card issuance and lifecycle maintenance in accordance with established procedures and controls.

10.2.5.1.6
(03-11-2024)
Terms/Definitions/ Acronyms

(1) **Access** - The permissions granted to employees and contractor employees 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 controlled facility or space, and to login to IRS systems with approved credentials.

Note: For additional information related to facility access, see IRM 10.2.18, Physical Access Control.

(2) **Alpha Files** - Alphabetized files that are stored in the local security office that may include various ID media forms.

(3) **Card Stock** - Blank cards that have no picture that are stored in a lockable cabinet in the FMSS security office.

(4) **Compromised** - ID media in the possession of an unauthorized user or ID cards believed to be tampered with including unauthorized physical alterations or hacked.

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

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

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

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

(7) **Escorted Access** - Access given to an individual (such as a contractor employee, visitor, or vendor) who is not approved for staff-like access and must be accompanied by a "qualified escort" during work performance and/or entry and movement throughout the facility.

Note: For additional information related to escorted access, see IRM 10.2.18, Physical Access Control.

(8) **ID Card** - A form of ID media that may include the bearer's photograph, name, agency affiliation, and card number, that verifies the identity of the bearer and may designate the type of authorized access granted.

(9) **ID Card Designations** - Verbiage that appears on ID cards that indicates a specified privilege or level of physical access, including concealed weapon, federal emergency response official, visitor or escort only.

(10) **ID Media** - IRS ID media includes any photo or non-photo ID card, pocket commission, or similar items, which contain the IRS name, seal, or symbol, that is issued to and displayed by the bearer.

(11) **IRS Employee** - a federal employee, employed by the IRS.

(12) **Limited Area** - A space or room to which access is limited to authorized personnel only.

(13) **Logical Access** - Access to IRS information systems or to Information Technology (IT) resources.

(14) **Lost ID Card** - ID cards that currently have no known location.

(15) **Non-Work Status** - A temporary non-pay status such as a seasonal or intermittent worker, extended Leave Without Pay (LWOP), extended Absence Without Leave (AWOL), furlough, suspension, military leave, or other non-pay status.

(16) **Physical Access Control (PAC) Card** - A photo ID card issued that verifies the identity of the bearer for facility access only.

(17) **Proxy/Access Cards** - Non-photo, electronic cards that work with the access control system to unlock a door or a similar structure, replacing a traditional key and lock.

(18) **Pseudonym** - A fictitious name. The use of a pseudonym is issued to an IRS employee for the protection of personal safety and the prevention of harm or danger.

Note: For additional information, see IRM 10.5.7, Use of Pseudonyms by IRS Employees.

(19) **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 individual who requires escorting, and with knowledge of the task or activity to be performed.

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

(20) **Recovered** - A classification for ID media returned to the manager or COR and forwarded to the local FMSS security office for final disposition.

(21) **Routine Access** - Access to facilities on a consistent basis, generally multiple times per week.

(22) **SmartID** - A photo ID card issued in accordance with HSPD-12 that verifies the identity of the bearer through visible and embedded biometric data. The SmartID card provides logical and facility access.

(23) **Staff-like Access** - Authorized unescorted access to IRS-owned or controlled facilities, IT systems, security items and products, or areas storing/processing SBU data as determined by Treasury/bureau officials. Staff-like access may be interim or final. Staff-like access is granted to an individual who is not an IRS employee and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.

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

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

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

(25) **Visitor** - A person seeking access to an IRS facility who has not been issued a SmartID or may not be in possession of a SmartID. Visitors may include contractor employees who have not been approved for staff-like access, other federal agency employees and contractors, the general public, and employees or contractor employees when then are not in possession of their ID card.

(26) **Visitor Management System (VMS) ID Cards** - ID cards that include the bearer's photograph and expiration date that will automatically erase the photograph once expiration date is reached. To obtain a VMS card, please contact the local security office.

(27) **Unrecoverable** - A classification for ID media not returned to the local FMSS security office, manager or COR after attempts have been made for its return.

Acronyms

Acronym	Definition
AD	Associate Director
AIM	Access and Identification Management

Acronym	Definition
AWOL	Absence Without Leave
CO	Contracting Officer
COR	Contracting Officer's Representative(s)
FIPS	Federal Information Processing Standards
FMSS	Facilities Management and Security Services
GRS	General Record Schedule
HR	Human Resource
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential and Access Management
ID	Identification
IT	Information Technology
ITM	Integrated Talent Management
LAK	Light Activation Kits
LWOP	Leave Without Pay
NARA	National Archives and Records Administration
OMB	Office of Management & Budget
PAC	Physical Access Control
PIV	Personal Identity Verification
SAMC	Situational Awareness Management Center
SBU	Sensitive But Unclassified
SCC	Separating Contractor Clearance
SEC	Separating Employee Clearance
SSC	Security Section Chief(s)
TM	Territory Manager
USC	United States Code
USPS	United States Postal Services
VMS	Visitor Management System

10.2.5.1.7
(03-11-2024)
Related Resources

(1) Document 12829, The General Records Schedules (GRS)

(2) Form 14604, Contractor Separation Checklist

(3) Form 3210, Document Transmittal

(4) Form 4589, Lost or Forgotten Identification (ID) Media Record

(5) Form 6662, Daily ID Card Inventory Report

(6) IRM 1.2.2, Servicewide Policies and Authorities

(7) IRM 1.17.7, Use of the Official IRS Seal, IRS Logo, Program Logos and Internal Logos

(8) IRM 1.22.3, Addressing and Packaging

(9) IRM 9.11.3, Investigative Property

(10) IRM 10.2.6, Pocket Commissions

(11) IRM 10.2.8, Incident Reporting

(12) IRM 10.2.14, Methods of Providing Protection

(13) IRM 10.2.18, Physical Access Control

(14) IRM 10.5.1.5.1, Clean Desk Policy

(15) IRM 10.5.7, Use of Pseudonyms by IRS Employees

(16) IRM 10.8.1, Policy and Guidance

(17) IRM 10.23.2, Contractor Investigations

10.2.5.2
(03-11-2024)
Authorized Use

(1) Only ID media issued in accordance with, or as referenced in this IRM section are authorized for use by IRS employees and contractor employees during performance of official duties. The issuance and use of pocket commissions is covered in IRM 10.2.6, Pocket Commissions, and enforcement badges in IRM 9.11.3, Investigative Property.

(2) IRS employees and contractor employees should take precautions to prevent loss, theft, or destruction of pocket commissions, ID cards, and enforcement badges. They are responsible for safeguarding their ID media on their person or in a locked container. ID media should never be left unattended in briefcases, unlocked desk drawers, automobiles, etc.

(3) No IRS employee or contractor employee may possess more than one IRS ID card. No IRS employee or contractor employee may be issued more than one ID card, unless otherwise authorized by the AD, Security.

(4) IRS employees and contractor employees must return all ID media on their last workday when they separate or terminate employment (resignation or retirement, transferring to another federal agency, removal, etc.).

(5) IRS employees and contractor employees must never copy or photograph their ID media, nor allow anyone to copy or photograph their ID media, as per 18 USC 701, Official badges, identification cards, other insignia.

(6) ID media may not be used for retirement mementos, honorary presentations, or similar purposes, except as prescribed in IRM 10.2.6, Pocket Commissions, and IRM 9.11.3, Investigative Property.

10.2.5.3
(04-28-2021)
Penalties

(1) See *18 USC 499: Military, naval, or official passes*

(2) See *18 USC 701: Official badges, identification cards, other insignia*

10.2.5.4
(03-11-2024)
Mailing ID Cards

(1) ID cards may be mailed when an ID card must be:

a. Transferred to another credentialing station, including non-IRS credentialing stations, or to a Light Activation Kit (LAK) station.
b. Returned to the local FMSS security office due to employee or contractor employee separation or placement in a non-work status.

(2) When mailing ID media:

a. Use traceable means such as the United States Postal Service (USPS) registered mail or with a tracking number. The tracking number must be sent to the package recipient once it is received from the mailing service.
b. Use a sealed envelope with the name of the receiving employee or contractor employee recorded on the face of the envelope. The sealed envelope containing the ID media must then be double wrapped for mailing.

Note: For additional information, see IRM 1.22.3, Addressing and Packaging.

c. The mailing package must be accompanied by a Form 3210, Document Transmittal, including the name of the package recipient, date sent, serial number, type of ID media, quantity of blank stock (if applicable), and cardholder's name (if applicable).
d. Form 3210 must be retained for use in ensuring the timely receipt of the transmitted items. The recipient must return the signed Form 3210 indicating receipt. A copy of the signed Form 3210, signifying receipt of the documents, must be retained in the local FMSS security office.

10.2.5.5
(03-11-2024)
Authorized ID Media

(1) The authorized forms of ID media approved for use by IRS employees, contractor employees, and visitors are as follows:

a. ID cards (photo and non-photo)
b. Pocket Commissions, in accordance with IRM 10.2.6, Pocket Commissions
c. Enforcement badges and Pocket Commissions in accordance with IRM 9.11.3, Investigative Property
d. Proxy/access cards
e. VMS ID cards

(2) IRS employees, contractor employees, and visitors may not display any form of ID cards associating them with the IRS except as referenced in this IRM unless otherwise officially authorized by the Chief, FMSS.

(3) Requests for the development of new or modification of existing ID cards, the method of use, assembly, or display, must be submitted to the FMSS AD, Security, for coordination and forwarding to the Chief, FMSS, for approval.

(4) The Chief, FMSS is the approving authority for any amendments to any type of IRS ID cards, unless otherwise indicated in this IRM.

(5) All other forms of ID media not specifically covered in this IRM, IRM 10.2.6, Pocket Commissions, or IRM 9.11.3, Investigative Property, are not authorized.

10.2.5.6
(03-11-2024)
Photo ID Cards

(1) Photo ID cards are only issued by the local credentialing office to employees and contractor employees who meet the eligibility requirements for staff-like access, as per IRM 10.2.18, Physical Access Control, IRM 10.23.2, Contractor Investigations, and require routine physical and/or logical access to IRS facilities and systems.

(2) Authorized photo ID cards are the SmartID, PAC cards, and VMS ID cards.

(3) PAC cards may be issued to individuals who meet the eligibility requirements for staff-like access and require routine physical access to IRS controlled facilities subject to the approval of Chief, Access & ID Management.

(4) Authorized personnel who require specified access or privilege must have ID designations on the front of the ID card in accordance with FIPS 201 guidance. The ID designations are as follows:

a. **Federal Emergency Response Official (FERO)**: Personnel designated as emergency responders.
b. **Concealed Weapon**: Personnel authorized to carry concealed weapons in conjunction with their official duties.
c. **Limited Area Access**: Personnel authorized to access limited areas, spaces and/or rooms.

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

(5) Employees must schedule an appointment at their local credentialing office to be issued a photo ID card.

(6) Contractor employees must schedule an appointment at their local credentialing office to be issued a photo ID card. The COR is responsible for ensuring that contractor employees meet the unescorted access eligibility requirements prior to obtaining the ID card and continue to meet eligibility to maintain unescorted access in accordance with IRM 10.2.18.

(7) Employees and contractor employees that require photo ID cards are required to have a photograph taken to provide an immediate visual verification of the bearer's identity. Employees and contractor employees must provide a neutral facial expression for the photo, where all facial muscles are in a relaxed state. Wearing hats, scarves, caps, or items that may obstruct the facial features are prohibited unless worn for reasons of religion or health. Exceptions must be approved by the local FMSS SSC and notated in the employee's identity record.

(8) Employees and contractor employees must ensure ID cards are in their possession when conducting official business. ID cards must be worn between the neck and waist and displayed visibly from the front when in IRS facilities.

(9) SmartID cards must be carried in an IRS issued holder to safeguard the ID card certificate. When the SmartID card is being utilized for work processes,

such as Single Sign-On, it's allowable to not have the card displayed if it's in the cardholder's physical possession at all times.

(10) Employees with an approved pseudonym, as prescribed in IRM 10.5.7, Use of Pseudonyms by IRS Employees, must be issued a SmartID card in their pseudonym name only. Previously issued ID cards must be recovered and returned to the local FMSS security office prior to the issuance of a new ID card. The pseudonym name must match on the SmartID card and the enforcement or non-enforcement pocket commission, if applicable.

10.2.5.6.1
(03-11-2024)
Replacement ID Cards

(1) Employees and contractor employees must contact their manager or COR to request a replacement card if the:

a. Current ID card has expired
b. ID card is lost, stolen, or compromised
c. Cardholder's name has changed
d. ID card is worn or damaged
e. Image of the cardholder no longer accurately depicts the cardholder

(2) Cardholders must immediately report lost, stolen, or compromised ID cards to:

a. Their manager or COR
b. The local FMSS security office by submitting Form 4589, Lost or Forgotten Identification (ID) Media Record
c. SAMC in accordance with IRM 10.2.8, Incident Reporting

(3) IRS employees and contractor employees who require a replacement ID card must schedule an appointment at their local credentialing office to be issued a replacement ID card.

(4) The COR is responsible for ensuring that contractor employees meet the unescorted access eligibility requirements at time of appointment.

(5) Local security offices must complete revocation procedures within 18 hours of notification of lost, stolen, or compromised ID cards or proxy cards. In emergency situations where there is suspicion the missing ID card could be misused, the local FMSS security office must take immediate action to disseminate the information to SAMC to prevent unauthorized access to IRS facilities and systems.

10.2.5.6.2
(03-11-2024)
Non-Photo ID Cards

(1) The authorized non-photo ID cards are Visitor and Visitor Escort Only. Individuals who require non-photo ID cards must have ID designations on the front of the ID card. The ID designations are as follows:

a. "V" in a red field – Visitor
b. "E" in a red field – Visitor Escort Only
c. "R" in a yellow field – Visitor Limited Area

(2) Visitors and federal or non-federal personnel who have met the eligibility requirements for staff-like access as set forth in IRM 10.2.18, Physical Access Control must be issued non-photo Visitor ID cards by the local FMSS security office for unescorted access.

(3) Visitors who have **not** met the eligibility requirements for staff-like access must:

a. Be escorted by a qualified escort, who must request their placement on the facility visitor access list in accordance with IRM 10.2.18.
b. Present a government or state issued photo ID card for identity verification.
c. Submit to facility entry screening procedures.
d. Be issued a non-photo Visitor Escort Only ID card.

(4) Limited Area Monitors will follow access procedures as set forth in IRM 10.2.18.

(5) Employees and contractor employees who report to IRS facilities without their IRS issued photo ID card must complete and submit Form 4589, Lost or Forgotten Identification (ID) Media Record to the local FMSS security office and must be issued a Visitor ID card if a SmartID replacement card is not available.

(6) Non-photo ID cards cannot be removed from the issuing facility and should never be used as access authorization to a facility. Non-photo ID cards must be returned to local FMSS security office or guard post by the individual assigned the card when the individual departs the facility or controlled area.

(7) Contractor employees who have been denied final staff-like access by Personnel Security, Human Capital Office cannot be allowed entry.

10.2.5.6.3
(03-11-2024)
Proxy/Access Cards

(1) IRS employees and contractor employees who require a proxy/access card must meet the access eligibility requirements per IRM 10.2.18, Physical Access Control, and schedule an appointment at their local FMSS security office.

(2) Proxy/access cards must be issued by the local FMSS security office for applicable IRS controlled facilities or space. Proxy/access cards must be returned to the local FMSS security office upon separation or non-work status by the individual assigned the card or their manager.

Note: Proxy/access cards are not transferable.

(3) The local security office is responsible for assigning access and timely removing access from the local access control system upon separation or non-work status in accordance with IRM 10.2.5.7(2), Recovery of ID Media, and IRM 10.2.5.8(4), Records and Accountability.

10.2.5.7
(03-11-2024)
Recovery of ID Media

(1) All issued ID cards must be recovered and returned to the local FMSS security office when employees or contractor employees:

a. Receive replacement ID cards.
b. Separate and terminate employment (resignation or retirement, transferring to another federal agency, etc.).
c. Are placed in non-work status.
d. ID card designation is no longer valid.

Note: Recovery of pocket commissions must follow procedures in IRM 10.2.6, Pocket Commissions.

(2) The local FMSS security office is responsible for ensuring all issued VMS ID cards are recovered and returned to the local FMSS security office when the visitor's access is no longer authorized.

(3) All ID media items must be recovered on the employee's or contractor employee's last workday prior to separating or terminating employment with the IRS.

(4) The manager or COR are responsible for initiating the process of recovering the ID media items for separated employees and contractor employees and must attempt to contact the employee or contractor employee (including tracked letter, documented phone call, etc.) to recover the ID media items, prior to filing a SAMC report.

(5) The local FMSS security office is responsible for verifying the termination of ID cards for separating employees and contractor employees and must:

a. Terminate ID cards that are not systematically terminated in the SmartID card management system within three business days of notification.
b. Complete card destruction for all recovered cards within three business days of notification.
c. Verify ID card destruction for all recovered ID cards in the SmartID card management system.

(6) The manager or COR are responsible for ensuring that all recovered ID cards are returned to the local FMSS security office no later than one business day after the effective date of the separation with Form 3210, Document Transmittal, either in person or if being mailed, post marked by the next business day.

(7) The manager is responsible for the timely completion of all recovery and separation procedures for employees. The manager is required to use the HRConnect – SEC module to indicate ID media recovery status as recovered or unrecoverable on the employee's last workday.

(8) If the manager is unable to recover the ID media item(s), the manager must:

a. File a SAMC report with written explanation detailing the circumstances of non-recovery prior to completing the SEC module in HRConnect.
b. Update the SEC module to indicate the ID media as unrecoverable including the written explanation detailing the circumstances of non-recovery and the SAMC report number.
c. Provide the SAMC report number to the local FMSS security office no later than one business day after effective date of separation via email or hard copy with Form 3210, Document Transmittal.

Note: For additional guidance, see IRM 10.2.8, Incident Reporting.

(9) The COR's manager is responsible for the timely completion of all recovery and separation procedures for contractor employees. The manager or COR is required to complete and submit Form 14604, Contractor Separation Checklist, on the contractor employee's last workday and indicate the status of the ID media as recovered or unrecoverable.

When the manager or COR is unable to recover the ID media, the manager or COR must:

a. File a SAMC report with a written explanation detailing the circumstances of non-recovery, prior to completion of Form 14604, Contractor Separation Checklist.
b. Complete Form 14604, Contractor Separation Checklist, indicate the ID media as unrecoverable including the written explanation detailing the circumstances of non-recovery and the SAMC report number and attach the checklist to the HRConnect - SCC module for contractors.
c. Provide the SAMC report number to the local FMSS security office no later than one business day after effective date of separation via email or hard copy with Form 3210, Document Transmittal.

Note: For additional guidance, see IRM 10.2.8, Incident Reporting.

(10) Employees and contractor employees should refer to IRM 10.2.5.3, Penalties, for the penalties of failing to return ID media or the misuse ID media.

10.2.5.8
(03-11-2024)
Records and Accountability

(1) Unauthorized personnel must not have access to the ID card stock, supplies, or equipment to maintain the validity and reliability of ID media. Local FMSS security staff must maintain all ID card stock, supplies, alpha files, and equipment in a lockable cabinet. Credentialing stations must adhere to clean desk policy per IRM 10.5.1.5.1, Clean Desk Policy.

(2) The local FMSS security office must maintain an alpha file for individuals who have the following forms:

a. Form 4589, Lost or Forgotten Identification (ID) Media Record
b. SAMC reports completed by local FMSS security office
c. Written explanations by the manager or COR for all unrecoverable ID media
d. Form 3210, Document Transmittal

(3) Alpha files must be maintained by the local FMSS security office for a minimum of three years after the date of the form.

Note: Refer to Document 12829, The General Records Schedules (GRS) for the approved records retention and disposition authority to ensure records, in hard copy and electronic format, are appropriately managed, retained and archived to prevent inadvertent/unlawful destruction of records. Refer to GRS 5.6-Security Management Records, Item 20-Key and card access accountability records; GRS 5.6-Security Records, Item 120-Personal identification credentials and cards; and GRS 5.6-Security Records, Item 130-Temporary and local facility identification and card access records, for the National Archives and Records Administration (NARA) approved retention and disposition.

(4) The local FMSS security office is responsible for completing the SAMC report for all unrecovered ID media no later than 30 days after separation of an employee or contractor where the manager, COR, or manager of the COR has not completed the SAMC report.

(5) The local FMSS security office must complete a daily inventory of all non-photo ID cards. The local FMSS security office must annotate the results of the daily audit of each non-photo ID on Form 6662, Daily ID Card Inventory Report. Form 6662 must be maintained for a minimum of three years at the local FMSS security office.