TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Were Made in Installing Card Readers but Physical Security Deficiencies Remain

September 22, 2026

Report Number: 2026-200-051

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Improvements Were Made in Installing Card Readers but Physical Security Deficiencies Remain

Final Audit Report issued on September 22, 2026 **Report Number 2026-200-051**

Why TIGTA Did This Audit

All government employees and contractors are required to use standard identification to gain physical access to federally controlled sites.

The Enterprise Access Control System (EPACS) is the Internal Revenue Service's (IRS) solution to address federal physical access and authentication requirements at IRS sites. The IRS uses the Personal Identify Verification (PIV) card as its standard form of identification. Card readers are located at the doors of IRS sites. Standard card readers only require a scanned PIV card to gain access. Multi-factor authentication card readers require both a scanned PIV card and a personal identification number unique to the card holder to gain access.

In September 2023, we reported that physical access controls were not fully implemented and audit logs were not reviewed or monitored. We made seven recommendations to improve physical access controls at IRS sites and EPACS account management.

We evaluated the IRS's continued deployment of the EPACS and followed up on recommendations from our prior audit to determine if they were effectively implemented.

Impact on Tax Administration

When physical access controls are not effectively implemented, there is an increased risk of unauthorized entry to IRS sites, potentially leading to theft of taxpayer information, compromise of IRS's systems and networks, or physical harm to personnel.

What TIGTA Found

We found that some IRS employees continued to access IRS sites despite being on administrative leave. These employees were on administrative leave because they accepted a deferred resignation offer. Specifically, our review of 22,227 employees that accepted the offer determined that 2 percent (431 of 22,227) accessed IRS sites after the start of their administrative leave dates. These 431 employees did not have an apparent business reason for accessing IRS sites. When asked why this occurred, management could not provide an explanation.

In addition, we followed up on seven prior audit recommendations and found:

- Three recommendations were fully implemented. We did not identify additional concerns during this review.
- Three recommendations were implemented, but we found that additional actions were needed to fully address our concerns. We continued to find EPACS operator accounts that did not have the matching permissions and were not properly disabled in the entitlement system. In addition, we found alarms that did not appear in EPACS and were not timely investigated.
- One recommendation was not implemented. The recommendation was to ensure that all noncompliant card readers were replaced with federally compliant card readers and properly configured. However, implementation was delayed until October 2026. The IRS cited budget restrictions and staffing losses as the reason for the delay.

Finally, a Limited Area (*e.g.*, a mailroom at a large tax processing center) door was updated with a required multi-factor card reader after one of our site visits. Facilities Management and Security Services (FMSS) management at the site agreed that a multi-factor card reader was required and replaced the card reader in April 2026.

What TIGTA Recommended

We made four recommendations to the Chief, FMSS, to improve EPACS and physical security. This includes that FMSS work with the Chief, Human Capital Officer, to ensure that they receive daily notifications of employee separations, so that they use this information to systemically disable separating employees' cards. In addition, we recommended that FMSS coordinate with the Chief Information Officer to ensure that the planned tool to integrate the EPACS with the IRS's entitlement systems is implemented.

The IRS agreed with all four recommendations and stated that it either has implemented or plans to implement corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 22, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Were Made in Installing Card Readers but Physical Security Deficiencies Remain (Audit No.: 2026200002)

This report presents the results of our review to evaluate the continuous deployment of the Enterprise Physical Access Control System, including physical access controls, and determine whether recommendations from a prior audit were effectively implemented.[1] This review is part of our Fiscal Year 2026 Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data.*

Management's complete response to the draft report is included in Appendix II. If you have any questions, please contact me or Linna K. Hung, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] TIGTA, Report No. 2023-20-062, *The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement* (September 2023).

Table of Contents

Background

All government employees and contractors are required to use standard identification to gain physical access to federally controlled sites.[1] The National Institute of Standards and Technology outlines the authentication factors needed to access each protected area of a facility.[2] The Enterprise Physical Access Control System (EPACS) is the IRS's solution to address federal physical access and authentication requirements at IRS sites.

The IRS uses the Personal Identify Verification (PIV) card as its standard form of identification. EPACS authenticates an employee's PIV card when presented to a card reader. Card readers are located at the doors of IRS sites. A specialized team within the IRS's Facilities Management and Security Services (FMSS) organization is responsible for the installation, operation, and management of the EPACS and card readers. As of May 2026, FMSS management reported that card readers were installed at 79 percent (329 of 417) of required sites. The remaining 21 percent (88 of 417) sites are estimated to be completed by March 2028, depending on funding.[3]

According to FMSS management, employees are granted general site access to their assigned IRS locations. General access includes common areas, such as break rooms. In addition, site specific credentials may be granted based on the employee's role and requirements of their job. Some examples include access to Limited Areas, such as mailrooms and server rooms. Business Unit managers must sign a form approving the Limited Area access before FMSS grants access. These managers are also required to review the continued need for access to Limited Areas monthly and must notify FMSS if access needs to be removed. FMSS is also responsible for disabling PIV cards after receiving notification that an employee separated from the IRS.

Standard card readers require a scanned PIV card to gain access. Multi-factor authentication card readers require both a scanned PIV card and a personal identification number unique to the PIV card holder to gain access. IRS policy requires that Limited Areas have multi-factor authentication card readers to gain access. Figure 1 provides images of a PIV card, an EPACS standard card reader, and an EPACS multi-factor authentication card reader.

[1] Department of Homeland Security, Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004).

[2] National Institute of Standards and Technology, Special Publication 800-116, *Guidelines for the Use PIV Credentials in Facility Access* (June 2018). See Appendix II for a glossary of terms.

[3] The majority of the remaining sites were rated as a lower security risk by the IRS.

Figure 1: PIV Card and EPACS Card Readers

Source: Left: General Services Administration. Center: EPACS standard card reader (FMSS image). Right: EPACS multi-factor authentication card reader (FMSS image).

In September 2023, we reported on the implementation of EPACS security controls.[4] We evaluated the IRS's deployment and security controls of the EPACS and found that improvements were needed. For example, we found that physical access controls were not fully implemented and audit logs were not reviewed or monitored. We made seven recommendations to improve physical access controls at IRS sites and EPACS account management. The IRS agreed with six of the seven recommendations and partially agreed with one. Our recommendations and the IRS's follow-up actions are discussed later in this report.

Deferred Resignation Programs

In January 2025, Presidential Memorandum, *"Return to In Person Work,"* required all federal employees, within the Executive Branch, to return to in person work at assigned offices on a full-time basis.[5] In addition, the IRS began reducing the overall size of its workforce through the Deferred Resignation Program (DRP) and the Treasury DRP. These programs allowed employees to voluntarily resign and generally be placed on administrative leave until September 30, 2025. If retiring, the retirement dates for participants of both programs had to occur before December 31, 2025.

Employees on administrative leave do not have a business reason for accessing IRS facilities. They are required to return their PIV cards and have their site access disabled in EPACS before being placed on administrative leave. Unauthorized access can lead to disclosure of taxpayer information, which undermines public trust in the IRS's ability to safeguard confidential tax information.

[4] TIGTA, Report No. 2023-20-062, *The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement* (September 2023).

[5] *Return to In-Person Work*, 90 Fed. Reg. 8251 (January 20, 2025).

Results of Review

Some Employees Who Took a Deferred Resignation Continued to Access IRS Sites

Our review of EPACS access logs for 22,227 participants of DRPs determined that 2 percent (431 of 22,227) accessed IRS sites after the start of their administrative leave.[6] These 431 employees did not have an apparent business reason for accessing IRS sites. When asked why this occurred, management could not provide an explanation. As previously stated, employees on administrative leave should have had their access disabled. The access logs did not indicate that any of the remaining 21,796 participants accessed an IRS site after the start of their administrative leave date.

IRS guidance required participants of DRPs to return their PIV cards and IRS assets (*e.g.*, computer equipment) upon their administrative leave date. System access should also be disabled for these employees. We have two concurrent reviews of processes related to DRP participants. These reviews are evaluating:

- Whether the IRS took appropriate actions to ensure that access to sensitive systems is timely removed.
- The IRS's oversight and management of its information technology asset inventory for separated employees, including those who participated in a DRP.

Local FMSS security teams are required to disable PIV cards for separating employees within three business days of receiving notification from the employee's manager. FMSS management officials stated they were unable to handle the large volumes resulting from the DRPs because they relied on a manual process to disable access. As a result, not all participants' PIV cards were disabled.

The IRS recognized a need for a more efficient process because of the unprecedented volume of probationary employees who were terminated. In February 2025, FMSS developed an interim tool to disable access for probationary employees who were terminated. In July 2025, FMSS started using this tool to disable PIV cards for DRP participants based on weekly notifications from the Human Capital Office. The tool was used to disable PIV cards for probationary employees and DRP participants. However, FMSS does not use the tool for all employee separations.

FMSS currently relies on manual review to identify separated employees, which is subject to human error. Using the Human Capital Office's notification process and the tool created by FMSS for all employee separations is a more effective physical security control. This reduces the risk of human error that comes with manual review and disablement.

Failure to deactivate PIV cards for employees that no longer have a need to access an IRS site increases the risk of unauthorized entry, as we identified. This can potentially lead to theft of

[6] We identified these 22,000 employees based upon the employee reporting a DRP specific time and attendance code through December 2025. TIGTA's Office of Inspections and Evaluations reported nearly 21,500 employees through May 2025. The minor difference can primarily be attributed to timing.

taxpayer information, compromise of IRS's systems and networks, or physical harm to IRS employees.

The Chief, FMSS, should:

Recommendation 1: Coordinate with the Chief, Human Capital Officer, to ensure that FMSS receives daily notifications of employee separations so that FMSS can use or update its existing tool to systemically disable separating employees PIV cards.

> **Management's Response:** IRS management agreed with this recommendation and stated that it had deployed a configuration change that systemically disables separated employee and contractor PIV cards on a daily basis.

Recommendation 2: Verify that PIV card access has been disabled for the 431 DRP participants we identified.

> **Management's Response:** IRS management agreed with this recommendation and stated that it compared the list of DRP participants to both EPACS and Treasury credential records to confirm that PIV card access was disabled for participants that are not active employees or contractors.

Some Prior Audit Recommendations Were Not Fully Addressed

As previously discussed, in September 2023, we reported that EPACS physical security controls needed improvement. During this audit, we followed up on all seven recommendations and found:

- Three recommendations were fully implemented by the IRS. We did not identify additional concerns during this review. We found that:
  - The IRS completed the audit worksheet so that audit logs can be monitored and reviewed by Cybersecurity. We verified that the Cybersecurity function is capturing audit logs in the audit logging tool. They are also monitoring and reviewing the audit logs.
  - The IRS determined the cause for an inoperable alarm. We verified that the IRS replaced the inoperable card reader.
  - The IRS addressed issues with a door not recording actionable alarms in EPACS. We verified that the alarm is working properly.
- Three recommendations were implemented according to the IRS. However, we found that additional actions are needed to fully address our concerns. These recommendations are detailed in Figure 2 below.
- One recommendation has not been implemented. The recommendation was to ensure that all noncompliant card readers were replaced with federally compliant card readers and properly configured. However, it has been delayed until October 2026. FMSS cited budget restrictions and staffing losses as the reason for the delay. As a result, we were unable to assess the IRS's planned corrective action.

Figure 2 shows the additional actions needed in response to our prior findings and recommendations.

Figure 2: Prior Recommendations Where Additional Action Is Needed

Finding/Recommendation	Actions Taken	Additional Action Needed
EPACS operator accounts did not have matching permissions and were not properly disabled in the entitlement system. Operators have access to real-time information to administer credentials and physical access to IRS sites. **Recommendation 1 (page 4):** Update guidance to provide clarity on the specific entitlements needed and how to disable accounts.	The IRS updated the guidance in August 2024 and again in March 2026.	Our review of the updated guidance found that it addressed the specific entitlements and how to disable accounts. However, as of February 2026, we continued to find EPACS operator accounts that did not have the matching permissions and were not properly disabled in the entitlement system. During this review, FMSS agreed that additional action was needed. FMSS plans to implement an automated tool by the end of Fiscal Year 2026 to interface between EPACS and the entitlement system to ensure that effective controls are in place.
Alarms did not always appear in the EPACS Event Viewer or they were not timely addressed. **Recommendation 6 (page 10):** Establish a process to timely respond to actionable alarms.	The IRS issued a new Standard Operating Procedure (SOP). In addition, FMSS developed the *EPACS Event Dictionary* to assist physical security specialists in identifying actionable alarm event types.	Our review of the new SOP found that it addressed the timelines for responding to alarms. However, as of November 2025, we continued to find alarms that did not appear in EPACS and were not timely investigated. For example, our site visits identified at least 23 doors that had forced entry alarms due to mechanical and hardware issues. These were not investigated within the established timelines. During this review, FMSS agreed that additional action was needed. FMSS plans to implement procedures to ensure that accountability controls are put in place to timely address actionable alarms.
The data in the Door Group Design Document and the EPACS did not always align.[7] **Recommendation 7 (page 13):** Implement a process to ensure that the design document and the EPACS are updated when changes occur.	The IRS issued a new SOP that outlines the process to ensure that the Door Group Design Document and the EPACS have the correct information when the installation of EPACS is completed.	Our review of the new SOP found that it does not provide instructions for updating the design document when changes occur (such as removals of card readers). The SOP only covers installations, which is not sufficient. As a result, the IRS continues to have errors on card readers and door naming conventions. For example, the IRS reported that 13 doors had card readers removed or not installed without updating the design document. FMSS submitted service tickets to update the design document and EPACS. **Management Action:** In June 2026, FMSS updated guidance to also reflect instructions for updating the Door Group Design Document when a card reader is removed.

Source: Summary of prior audit recommendations, IRS corrective actions, and audit testing.

[7] The Door Group Design Document is the document of record for doors and card reader programming. This document captures both the physical location of reader location and the specific programming for each card reader.

The Chief, FMSS, should:

Recommendation 3: Coordinate with the Chief Information Officer to ensure that the planned tool to integrate the EPACS with the IRS's entitlement systems is implemented so that operator accounts have the appropriate entitlements for their roles and accounts and are properly disabled.

> **Management's Response:** IRS management agreed with this recommendation and plans to implement a manual monthly reconciliation process so that operator accounts have the appropriate entitlements for their roles and accounts and are properly disabled.

Recommendation 4: Ensure that procedures are updated to add accountability controls so that actionable alarms are responded to timely.

> **Management's Response:** IRS management agreed with this recommendation and stated that it had issued a communication to all security section chiefs that actionable alarm reports for all EPACS-connected facilities must be reviewed and certified monthly.

A Limited Area Door Was Updated With a Required Multi-Factor Card Reader

During a site visit at an IRS office, in November 2025, we observed that a restricted area (*i.e.*, mailroom at a large tax processing center) had only a single-factor authentication card reader installed. IRS policy requires that Limited Areas have multi-factor authentication card readers to gain access to those areas.

Failure to implement a multi-factor authentication card reader increases the risk of unauthorized individuals gaining access to the mailroom using lost or stolen PIV cards potentially leading to theft or compromising taxpayer information. IRS tax processing centers receive and process sensitive taxpayer information. For example, the mailroom contains paper tax returns with Social Security Numbers and bank account information from taxpayer payments.

Management Action: FMSS management at the site agreed that a multi-factor card reader was required. The IRS replaced the single-factor card reader with a multi-factor card reader in April 2026.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the continuous deployment of the EPACS, including physical access controls, and determine whether recommendations from the prior audit were effectively implemented. To accomplish our objective, we:

- Evaluated the EPACS implementation status by interviewing FMSS management and obtaining and reviewing the EPACS status report.
- Determined whether DRP participants gained access to IRS sites based upon IRS time and attendance system data and EPACS access data.
- Determined if the IRS adequately addressed all seven prior audit recommendations.
- Conducted site visits to evaluate various physical security controls.

Performance of This Review

This review was performed at IRS offices in Kansas City, Missouri, Fresno, California, and Detroit, Michigan during the period November 2025 through June 2026. We also obtained information from the FMSS and Cybersecurity functions located in Lanham, Maryland, and Kearneysville, West Virginia. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

We performed tests to assess the reliability of data from the IRS's time and attendance system, the EPACS access logs, and the IRS's entitlement system. We evaluated the data by 1) reviewing existing information about the data and the system that produced them, 2) reviewing required data fields, and 3) reviewing the data for completeness and accuracy. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objectives: EPACS Physical Security Operations Guide for logical controls and IRS policies related to logical and physical security controls. We evaluated these controls through interviews with personnel from the FMSS and the Information Technology organizations and reviews of relevant documentation provided by the IRS. We also conducted walkthroughs and tested EPACS card readers at selected sites.

Appendix II

Management's Response to the Draft Report

CHIEF
FACILITIES MANAGEMENT &
SECURITY SERVICES

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 24, 2026

MEMORANDUM FOR DIANA TENGESDAL
Deputy Inspector General for Audit

FROM: John M. Pekarik
Acting Chief, Facilities Management & Security Services

SUBJECT: Draft Audit Report – Improvements Were Made in Installing Card Readers; However, Physical Security Deficiencies Remain (Audit No.: 2026200002)

Thank you for the opportunity to review and comment on the draft audit report. We appreciate that your report acknowledged we deployed electronic physical access control systems to additional sites and addressed recommendations from the prior audit. Facilities Management and Security Services (FMSS) remains committed to the safety and security of our facilities and the employees and taxpayer information they contain. Your recommendations will assist us in our efforts.

The deferred resignation program (DRP) presented the Internal Revenue Service (IRS) with unique challenges in managing facility access. At the time of the DRP, the IRS policy did not require the collection of personal identity verification (PIV) cards or the termination of facility access for employees on administrative leave since administrative leave is not a separation. The IRS quickly issued guidance to employees and managers on procedures for DRP employees to return equipment and PIV cards. However, recovering government equipment proved challenging when employees and managers were not co-located, administrative leave dates changed after employees were accepted into the program, and managers departed before completing the required separation processes.

As noted in the report, 98% of DRP participants did not access an IRS facility after reporting DRP-specific administrative leave. This result affirms that the IRS' actions to quickly implement a tool to revoke physical access successfully mitigated the risk of unauthorized access. The analysis used to identify DRP participants who accessed an IRS facility may include instances in which employees inadvertently used an incorrect administrative time code or were recalled to perform work after initially being placed on administrative leave. We continued to collect and analyze available data for the remaining 431 DRP participants (2%) and

determined that approximately 300 of these employees accessed an IRS facility to return government equipment, including Personal Identity Verification (PIV) cards, or the access occurred on or before the administrative leave date reported by Treasury or provided by the employee's manager.

Attached is our corrective action plan describing how we plan to address your recommendations.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-6983 or John.M.Pekarik@irs.gov or a member of your staff may contact Ross C. Sickler, the acting Director, FMSS Physical Security at Ross.C.Sickler@irs.gov.

Attachment

Attachment

Improvements Were Made in Installing Card Readers but Physical Security Deficiencies Remain
Audit No. 2026200002

RECOMMENDATION #1:
The Chief, FMSS, should coordinate with the Chief, Human Capital Officer, to ensure that FMSS receives daily notifications of employee separations so that FMSS can use or update its existing tool to systemically disable separating employees PIV cards.

CORRECTIVE ACTION:
The Internal Revenue Service (IRS) agrees with this recommendation. The Facilities Management and Security Services (FMSS) deployed a configuration change that systemically disables separated employee and contractor Personal Identity Verification (PIV) cards on a daily basis.

IMPLEMENTATION DATE:
Implemented July 15, 2026

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION #2:
The Chief, FMSS, should verify that PIV card access has been disabled for the 431 DRP participants we identified.

CORRECTIVE ACTION:
The IRS agrees with this recommendation. The FMSS compared the list of 431 deferred resignation program (DRP) participants to both Enterprise Physical Access Control System (EPACS) and Treasury credential records to confirm that PIV card access is disabled for participants that are not active employees or contractors.

IMPLEMENTATION DATE:
Implemented July 29, 2026

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION #3:
The Chief, FMSS, should coordinate with the Chief Information Officer to ensure that the planned tool to integrate the EPACS with the IRS's entitlement systems is implemented so that operator accounts have the appropriate entitlements for their roles and accounts and are properly disabled.

CORRECTIVE ACTION:
The IRS agrees with this recommendation. The FMSS will implement a manual monthly reconciliation process so that operator accounts have the appropriate entitlements for their roles and accounts and are properly disabled.

IMPLEMENTATION DATE:
November 15, 2026

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor these corrective actions as part of our internal management system of controls.

RECOMMENDATION #4:
The Chief, FMSS, should ensure that procedures are updated to add accountability controls so that actionable alarms are responded to timely.

CORRECTIVE ACTION:
The IRS agrees with this recommendation. The FMSS issued a communication to all security section chiefs that effective immediately, actionable alarm reports for all EPACS-connected facilities must be reviewed and certified monthly.

IMPLEMENTATION DATE:
Implemented June 23, 2026

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
N/A

Appendix III

Glossary of Terms

Term	Definition
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Business Unit	A title for IRS offices and organizations such as the Office of Appeals, the Office of Professional Responsibility, and the Information Technology organization.
Enterprise Physical Access Control System	System used to selectively authorize or restrict access to IRS facilities or spaces.
Facilities Management and Security Services	IRS organization that provides facility management and physical security solutions.
Limited Area	A security area where access is limited to authorized personnel by a multi-factor authentication mechanism.
Multi-Factor Authentication	Verifying the identity of a user, process, or device using two or more factors to achieve authentication, often as a prerequisite to allowing access to resources in an information system. Factors include: 1) something you know, (*e.g.*, password/Personal Identification Number); 2) something you have, (*e.g.*, cryptographic identification device, token); or 3) something you are, (*e.g.*, biometric).
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Personal Identity Verification Card	A physical artifact (*e.g.*, identity card, "smart" card) issued to an individual that contains stored identity credentials (*e.g.*, photograph, cryptographic keys, digitized fingerprint representation) such that the claimed identity of the cardholder may be verified against the stored credentials by another person or an automated process.
Single-Factor Authentication	A characteristic of an authentication system or a token that uses one of the three authentication factors to achieve authentication – something you know, something you have, or something you are.

Appendix IV

Abbreviations

DRP	Deferred Resignation Program
EPACS	Enterprise Physical Access Control System
FMSS	Facilities Management and Security Services
IRS	Internal Revenue Service
PIV	Personal Identify Verification
SOP	Standard Operating Procedure
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at
TIGTACommunications@tigta.treas.gov.

Information you provide is confidential, and you may remain anonymous.