TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement

September 27, 2023

Report Number: 2023-20-062

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

HIGHLIGHTS: The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement

Final Audit Report issued on September 27, 2023 **Report Number 2023-20-062**

Why TIGTA Did This Audit

All Government employees and contractors are required to use standard identification to gain physical access to Federally controlled facilities. The Enterprise Physical Access Control System (EPACS) is the IRS's solution to address the Federal physical access control requirements.

The EPACS provides electronic physical access control to IRS facilities by authenticating employees' SmartID when presented to a card reader at a perimeter door or at controlled and limited access doors inside IRS protected areas.

The EPACS also allows designated EPACS operators access to real-time system information to administer employee credentials and control physical access to facilities. EPACS operator's permissions are granted access through the Business Entitlement Access Request System (BEARS).

This audit was initiated to evaluate the deployment of the EPACS and security controls over the system.

Impact on Tax Administration

When audit logs are not regularly reviewed and monitored, inappropriate activities may not be identified in a timely manner. Without adequate access controls, sensitive equipment and information may be at risk of unauthorized access or disclosure.

What TIGTA Found

The methodology used to select and prioritize IRS facilities for the EPACS installation was effective and the planning tool used to guide the installation project from planning to completion was working as intended.

However, TIGTA's review of 81 EPACS operator accounts determined that operator account management is not effective. For example, 14 (17 percent) of 81 EPACS operator roles assigned in the EPACS did not have a matching entitlement in the BEARS. Specifically, privileged EPACS operator account roles are not consistently applied, some EPACS operator roles are changed without matching entitlements, the administrator role does not require approval through the BEARS, and the inactivity control did not always work as intended. Further, audit logs were not reviewed or monitored.

In addition, TIGTA conducted walkthroughs at eight IRS facilities to evaluate physical access controls including card readers, notifications from actionable alarms, user identification, visitor logs, and door classification documentation. TIGTA determined that three facilities had protected areas with incorrect card readers installed. One facility contained 24 two-factor authentication card readers that were not configured for two-factor authentication. IRS management subsequently stated that there are an additional 1,262 of the same type of noncompliant card readers at other locations. Another facility contained a two-factor authentication card reader that was broken.

Further, visitor access controls, signage, appropriate SmartID designations, and the door classification in the design document was missing, incorrect, or incomplete. During our review, the IRS updated the Internal Revenue Manual to revise the security classification of some areas.

Finally, the IRS implemented recommendations from a prior audit to ensure that a computer room is secured with a multi-factor authentication card reader.

What TIGTA Recommended

TIGTA made seven recommendations including that the Chief, Facilities Management and Security Services (FMSS), should ensure that the EPACS Operations Guide is updated, all protected areas are secured with Federally compliant and properly configured card readers, resolve the cause for the inoperable alarm, and implement a plan to timely address actionable alarms. Also, the Chief Information Officer should complete requirements for audit log reviews.

The IRS agreed with six of the seven recommendations and partially agreed with one recommendation. The Chief, FMSS, plans to implement a new Guide, replace all noncompliant card readers with compliant ones and properly configure them, and ensure that the design document and the EPACS have correct information. Also, the Chief Information Officer in partnership with FMSS plans to complete requirements to enable audit logs to be monitored and reviewed.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 27, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement (Audit # 202220023)

This report presents the results of our review to evaluate the deployment of the Enterprise Physical Access Control System and security controls over the system. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

All Government employees and contractors are required to use standard identification to gain physical access to Federally controlled facilities.[1] The National Institute of Standards and Technology (NIST) outlines the number of authentication factors needed to access each protected area of a facility.[2]

The Enterprise Physical Access Control System (EPACS) is the Internal Revenue Service's (IRS) solution to address Federal physical access and authentication requirements. The EPACS provides electronic physical access control to IRS facilities by authenticating employees' SmartID when presented to a card reader at a perimeter door or at controlled or limited access doors inside IRS areas. The EPACS allows designated EPACS operators access to real-time system information to administer employee and contractor credentials and control physical access to facilities. The EPACS operator's permissions are granted through the Business Entitlement Access Request System (BEARS).

The Access Control Management (ACM) team within the Facilities Management and Security Services (FMSS) organization is responsible for the installation, operation, and management of the EPACS. According to FMSS management, the ACM team follows physical access policy in compliance with all applicable Federal directives and aligns with IRS and FMSS Strategic Plans to protect employees and facilities. The ACM team stated that it also has contractor support to assist with operations, software management, and installation of the EPACS.

Results of Review

Planning for the Installation of the Enterprise Physical Access Control System Was Adequate

We evaluated the planning for the installation of the EPACS at IRS facilities by reviewing the process to select and prioritize the sites requiring installation and the tools used to guide the project from beginning to end. The ACM team uses a database containing a consolidated list of IRS facilities to manage the inventory of buildings requiring EPACS installation. The ACM team prioritized the list by Facility Security Level which is a security designation based on the characteristics of each facility, the Federal occupant, and the appropriate security measures that must be implemented. The IRS prioritized facilities that required Personal Identity Verification authentication as well as those facilities that did not already have a physical access system installed. However, as the project progressed, other considerations went into the prioritization, such as the completion of main campuses first and then the buildings around them, Federal requirements, and public safety.

[1] Department of Homeland Security, *Homeland Security Presidential Directive-12* (Aug. 27, 2004).

[2] NIST, Special Publication 800-116 Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access* (June 2018). See Appendix IV for a glossary of terms.

We obtained an EPACS project status report from July 2022 that contained 319 buildings requiring installation that included the location, security level designation, type of system install, or update needed, and project status. This inventory of buildings is validated annually due to the addition of new building leases, and expired building leases. We determined that the methodology used to select and prioritize IRS facilities for the EPACS installation was effective.

In addition, the IRS uses a planning tool to guide the installation project from planning to completion. The tool progresses from information gathering, including site surveys and reviews, to validating the equipment to be installed, and concludes with the Site Acceptance Testing. This testing occurs after the EPACS installation or upgrade to validate that each Standard Door Group and Master Door Group correctly defines card holder access to restricted areas and that the programming of the hardware and software properly functions. We reviewed the planning tool for all eight of the sites we visited and found that it was working as intended.

Although we found that the planning for the installation of the EPACS was adequate, IRS personnel stated that the EPACS installation completion date is dependent on future information technology funding.

Enterprise Physical Access Control System Operator Accounts Were Not Effectively Managed

We determined that the EPACS operator account management process was not effective. Figure 1 depicts the process for granting operators access to the EPACS.

Figure 1: Process for Granting Operators Access to the EPACS

Source: Treasury Inspector General for Tax Administration's analysis of the process for granting EPACS operator access. IT = Information Technology.

We obtained a list of 1,568 EPACS operator accounts, of which 766 accounts were active, 744 disabled, and 58 disabled due to 120 days of inactivity. We judgmentally selected a sample of 81 EPACS operator accounts for review.[3] We compared the roles for the 81 operator accounts to the entitlements in the BEARS to determine whether they were effectively managed. We determined that 14 (17 percent) of 81 EPACS operator roles did not have a matching entitlement in the BEARS. Specifically,

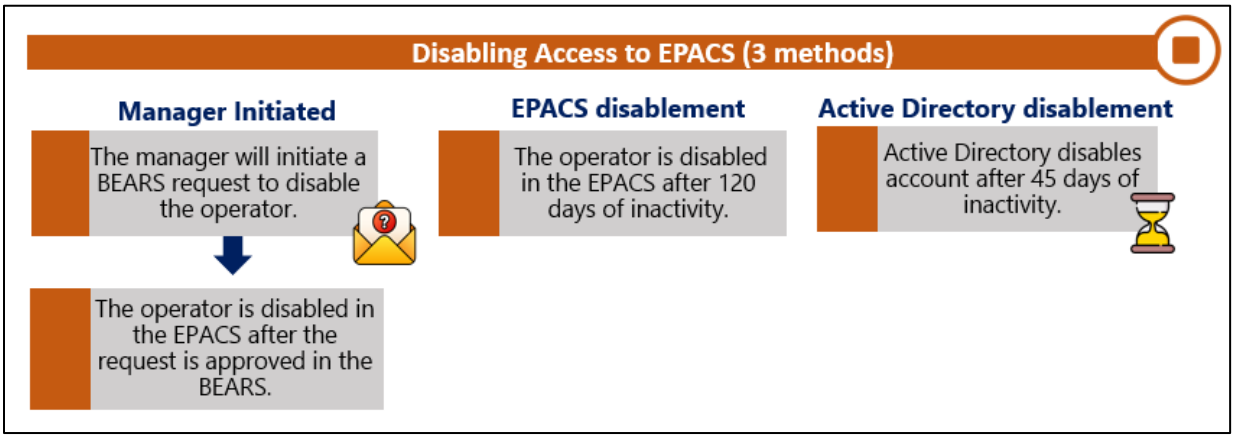
- **Privileged user account roles are not consistently applied between the EPACS and the BEARS.** The EPACS has a privileged role that enables the EPACS operator to modify physical access privileges for cardholders and the role includes elevated privileges to install hardware and software and troubleshoot access control issues within its local

[3] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

FMSS area. To assign this role, the EPACS operator requires two elevated privileged entitlements in the BEARS. We identified three instances where the user has this role in the EPACS but did not have the active elevated privileges in the BEARS. The inconsistency occurred because the ACM team does not have a validation process for these types of EPACS operator accounts. The IRS stated that they are in the process of ensuring that all EPACS operators assigned this role align with the elevated privileged entitlements in the BEARS.

- **EPACS operator roles are changed without matching entitlements.** We identified three instances where an EPACS operator's role changed in the EPACS; however, there was no matching entitlement in the BEARS. The ACM team explained that this occurred because the EPACS operator's manager did not ensure the change to the BEARS entitlement was properly submitted.
- **The administrator role does not require approval through the BEARS.** Our sample of EPACS operator accounts for review contained four operators with the administrator role which has all permissions as well as elevated privileges to perform full configuration activities for the EPACS. We determined that the role is assigned by the ACM team and does not follow the BEARS entitlement process. There is no formal process for granting, approving, and managing this role nor does it undergo the BEARS annual recertification process. The ACM team acknowledged that there should be a formal process to request the EPACS administrator role.
- **The inactivity control did not always work as intended.** Figure 2 depicts the process for disabling an EPACS operator's access to the EPACS.

Figure 2: Process for Disabling an EPACS Operator's Access to the EPACS



Source: Treasury Inspector General for Tax Administration's analysis of the EPACS operator access disabling process.

ACM management stated that an EPACS operator account is automatically locked after 120 days of inactivity (after the operator initially logs on to EPACS). However, we identified one instance of an operator account that was not disabled after 120 days of inactivity. This occurred because Active Directory disabled the operator's credentials, which prevented the ACM team from disabling the operator in the EPACS. We also identified three disabled operator accounts in the EPACS that had active entitlements in the BEARS. The EPACS system administrator manually disabled these three accounts

because the operators never logged on to EPACS to enable the EPACS 120-day inactivity automatic operator account lock.

The Internal Revenue Manual (IRM) requires that the creation, enabling, modification, disabling, or removal of a user account should be performed in accordance with IRS procedures.[4] The FMSS organization developed the EPACS Operations Guide that includes procedures for operator account management. The EPACS uses a role-based system to grant operator permissions. According to the EPACS Operations Guide, an operator must request access through the BEARS for the EPACS entitlements based on their role. The BEARS approval triggers the Information Technology organization to add the operator to Active Directory. After the operator's Active Directory account is setup, the ACM team is notified and will review the validity of the request and assign the operator the appropriate role(s) in the EPACS. To disable an operator's access, the employee's manager initiates the request in the BEARS. Once the disabled request is approved in the BEARS, the ACM team is notified via e-mail and will remove the employee's access to the EPACS. If an operator does not log into the EPACS after 120 days, the account is locked; however, their entitlement can remain active in the BEARS.

The operator account issues identified occurred because the EPACS Operations Guide does not clearly specify the procedures for granting and disabling accounts. ACM management stated that they are in the process of revising the EPACS Operations Guide. Without documented procedures in place, EPACS operators may be able to access more critical data, privileges, and application functions than they need which may lead to increased system security risks.

Recommendation 1: The Chief, FMSS, should update the EPACS Operations Guide to provide clarity on granting and disabling operator accounts and the specific entitlements that are required in the BEARS for all EPACS roles.

Management's Response: The IRS agreed with this recommendation. FMSS will develop and implement a new Velocity Operator Guide that will provide clarity on granting and disabling operator accounts and the specific entitlements that are required in the BEARS for all EPACS roles.

Audit Logs Are Not Reviewed or Monitored

The EPACS generates system logs that are stored in the logging and analytics repository tool; however, the logs are not being reviewed or monitored. The EPACS System Security Plan states that the Cybersecurity function is responsible for the review and analysis of audit records.[5] The Audit Worksheet documents the auditable and actionable events needed to facilitate the review of IRS information technology applications. The Audit Worksheet is completed by the Cybersecurity function's Enterprise Security Audit Trails team in collaboration with the business units, in this case, the ACM team. Once the Audit Worksheet is completed, the Cybersecurity function's Counter Insider Threat Operations team should begin reviewing and monitoring audit logs. According to Cybersecurity function personnel, they did not begin reviews of EPACS audit logs because the Audit Worksheet was not completed. Without regular reviewing and monitoring of the audit logs, inappropriate activities may not be identified in a timely manner.

[4] IRM 10.8.1 *Information Technology Security, Policy and Guidance* (Sept. 28, 2021).

[5] IRS, *IRS System Security Plan for Enterprise Physical Access Control System* (May 3, 2022).

Management Action: ACM management provided an e-mail stating that as of March 2023, the Enterprise Security Audit Trails team is hosting weekly working sessions with the EPACS team to update the Audit Worksheet.

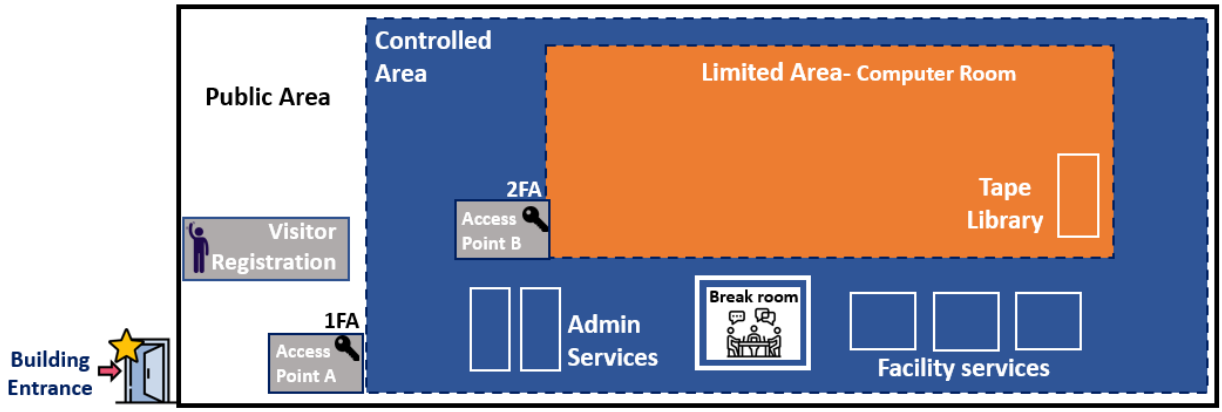
Recommendation 2: The Chief Information Officer should ensure that the Cybersecurity function's Enterprise Security Audit Trails team in collaboration with the ACM team prioritizes completing the Audit Worksheet so that the audit logs can be monitored and reviewed.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer in close partnership with FMSS will complete the Audit Worksheet to enable the audit logs to be monitored and reviewed.

Physical Access Controls Were Not Fully Implemented

We conducted eight site visits from August 2022 through December 2022 at buildings that completed the EPACS installation to evaluate the physical access security controls over Controlled and Limited Areas. Access to the Controlled Area of a secured facility requires a single authentication mechanism to ensure that only authorized personnel have access. Access to a Limited Area is granted to authorized personnel only and requires two-factor authentication to gain access.[6] Examples of Limited Areas include computer rooms, the receipt and control area, and mail/receipt rooms. Figure 3 is an example of a building with Controlled Areas (blue) and Limited Areas (orange).

Figure 3: A Building with Controlled and Limited Areas



Source: NIST Special Publication 800-116 Revision 1, Guidelines for the Use of Personal Identity Verification Credentials in Facility Access (June 2018) with modifications by the Treasury Inspector General for Tax Administration's Applied Research and Technology function to better replicate an IRS facility. 1FA = Single-factor authentication required to enter. 2FA = Two-factor authentication required to enter.

We evaluated card readers, notifications from actionable alarms, user identification, visitor logs, signage, and door classification documentation. We identified 85 physical security violations. Figure 4 provides a summary of these physical security violations.

[6] IRM 10.2.14, *Physical Security Program, Methods of Providing Protection* (Jan. 10, 2023).

Figure 4: Summary of Physical Security Violations by Site

Violation	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6	Site 7	Site 8	Totals by Violation
Incorrect Card Reader in the Limited Area	2			1				2	5
Two-factor Authentication Card Reader Not Configured as Two-factor		24							24
Card Reader Not Working			1						1
Alarm Did Not Appear in the EPACS						1			1
IRS Employee Without an "R" On SmartID Card Has Staff-like Access to Limited Areas[7]					1	1		1	3
No Limited Area Register (sign-in sheet) in Limited Area			2	2		2		4	10
Missing Limited Signage for Limited Areas	*		2	3			2	12	19
DGDD and/or EPACS Had Incorrect Information (*e.g.*, Card Reader Type, Door Name, NIST Classification)	5		8	3			1	5	22
Totals by Site	7	24	13	9	1	4	3	24	85

*Source: Results from the Treasury Inspector General for Tax Administration's onsite visits. * The Site 1 visit occurred during planning, and we did not include checking for signage in the limited areas. DGDD = Door Group Design Document.*

Limited Areas were secured with inadequate, improper configured, or inoperable card readers

We used the Door Group Design Document (hereafter referred to as the design document) to select a judgmental sample of Controlled and Limited Area doors to determine whether the correct card reader was installed and operational. The design document is used to map out all the components and elements of the door groups based on business rules for site access. All Controlled Areas we tested were properly secured by card readers that required a minimum of single-factor authentication to grant access. However, five (63 percent) of eight sites visited did not always have two-factor authentication card readers effectively installed to secure Limited Areas.

- **Incorrect card readers.** At Site 1, we tested 16 Limited Area doors to confirm they were adequately secured with two-factor authentication card readers. Two of the 16 Limited Area doors were not secured with two-factor authentication card readers. Instead, they were secured using single-factor authentication card readers.

[7] The "R" on the SmartID card of an employee or contractor indicates the person is authorized to access Limited Areas without an escort.

We found a similar issue at Site 8. We tested all 15 Limited Area doors and found two were not secured with two-factor authentication card readers. The first Limited Area stored printers and the Security Section Chief stated that they are considering changing the NIST classification to Controlled. Because printers are considered information technology equipment, we believe the Limited designation should remain, and a two-factor authentication card reader should be installed. When we discussed these issues with ACM management, they confirmed there is no verification process, including during the Site Acceptance Test, to validate that adequate devices are installed according to the Area's classification.

The second Limited Area door not secured with a two-factor authentication card reader had double doors with a single-factor authentication card reader that also required a key to unlock the doors. The design document reported that the door had a two-factor authentication card reader installed. The Security Section Chief stated that a two-factor authentication card reader could be installed if the double doors were replaced with a single door. The Security Section Chief stated that consideration would be given to moving the information technology equipment to another Limited Area that has a two-factor authentication card reader for cost savings purposes.

Management Action: At the time of our testing, the areas associated with those card readers were designated as Limited Areas. ACM management stated that a January 10, 2023, change to the IRM designated the IRS Computer Rooms (Martinsburg, Memphis, Kansas City, Fresno, Austin, Ogden, and Detroit) as Limited Areas.[8] Other information technology areas such as telecommunications equipment areas are now designated as Controlled Areas. Therefore, only the two card readers at Site 1 need to be replaced with two-factor card readers.[9]

At Site 4, we tested five Limited Area doors. One of the five Limited Areas was the mailroom which was listed on the design document as having a two-factor authentication card reader, but we observed that a single-factor authentication card reader was installed. The Physical Security Specialist explained that a two-factor authentication card reader was originally installed but the contractors working in the mailroom did not have the appropriate SmartID card to use and as a result, it was changed to a single-factor authentication card reader.

Management Action: After our site visit, the Physical Security Specialist verified that the contractor has the appropriate SmartID card and provided supporting evidence that a two-factor authentication card reader was reinstalled.

- **Card readers were not properly configured for two-factor authentication.** At Site 2, we tested nine of the 24 Limited Area doors in which the design document stated that two-factor authentication card readers were installed. The nine were configured for single-factor authentication only. The Physical Security Specialist stated that all two-factor authentication card readers were configured for single-factor authentication only. Therefore, we did not test the remaining 15 Limited Area doors. The ACM team stated that these two-factor authentication card readers were considered compliant with

[8] IRM 10.2.14 *Physical Security Program, Methods of Providing Protection* (Jan. 10, 2023).

[9] Site 1 is one of the seven designated Limited Areas.

Federal standards when they were installed in early 2020. According to ACM management, when it was time to begin the EPACS installation at this facility, the Federal requirements changed, and these card readers were no longer compliant with the updated Federal standards. The ACM team stated that the 24 card readers are scheduled to be upgraded by the end of Fiscal Year 2023. They also stated that there are an additional 1,262 of the same type of noncompliant card readers at other locations. All 1,286 readers are projected to be replaced by Fiscal Year 2026.

Management Action: At the time of our testing, the areas associated with the noncompliant card readers were designated as Limited Areas. ACM management stated that those areas are no longer classified as Limited Areas due to a change in the IRM requirement.[10] As a result of this change, those are now Controlled areas, which do not require two-factor authentication. The current IRM states that the IRS Computer Rooms (Martinsburg, Memphis, Kansas City, Fresno, Austin, Ogden, and Detroit) are designated Limited Areas.

- **A card reader was not operational.** During our visit to Site 3, we found a two-factor authentication card reader for a Limited Area door that was broken. The Physical Security Specialist explained that due to high usage, the card reader became inoperable.

  Management Action: We received confirmation from the IRS after our site visit that a service ticket was submitted to replace the card reader.

The NIST requires, at a minimum, single-factor authentication card readers for Controlled Areas and two-factor authentication card readers for Limited Areas.[11] Limited Areas require a Personal Identification Number pad equipped card reader (for two-factor authentication). The IRM also states that the EPACS should be used to secure Limited Areas, where feasible, to control entry.[12] A Limited Area is one in which access is limited to authorized personnel only. If the Limited Area is a small room or closet that is not always staffed and does not have an established staffed entry point, it must be properly secured. Without adequate access controls, the IRS is not compliant with Federal requirements and the sensitive equipment and information in the Limited Area may be at risk of unauthorized access or disclosure.

The Chief, FMSS, should:

Recommendation 3: Ensure that all 1,286 noncompliant card readers are replaced with Federally compliant card readers and are properly configured.

Management's Response: The IRS agreed with this recommendation. FMSS will ensure that all noncompliant card readers are replaced with Federally compliant card readers and are properly configured.

Recommendation 4: Replace the two single-factor authentication card readers in the Limited Areas at Site 1 and the broken two-factor authentication card reader at Site 3.

Management's Response: The IRS partially agreed with this recommendation. The IRS agreed with the recommendation regarding Site 3 and considers it complete. The

[10] IRM 10.2.14 *Physical Security Program, Methods of Providing Protection* (Jan. 10, 2023).
[11] NIST, Special Publication 800-116 Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access* (June 2018).
[12] IRM 10.2.14 *Methods of Providing Protection* (May 6, 2020).

Vendor was on site on October 25, 2022, and replaced the broken two-factor reader with a working two-factor reader. The Chief, FMSS, disagreed with the recommendation regarding Site 1. The Chief, FMSS, stated that due to the update to the IRM, the two Site 1 doors in question are now designated not as limited access areas but as controlled areas that require single factor authentication only.

Office of Audit Comment: Based on the revised NIST designation for the two Site 1 doors and the updated IRM, we concluded that the single-factor readers are now sufficient to meet the Federal requirements.

An alarm did not always appear in the EPACS viewer or was not timely addressed

FMSS management provided an Actionable Alarms Report, which lists more than 100 types of alarms generated by the EPACS that require action. Examples of alarms include forced entry at input (appears when circumventing the EPACS, such as using keys to open doors), Denied: Bad Personal Identification Number (good card), and Door Open Too Long. When alarms are generated, they appear in the EPACS Event Viewer and can be viewed by any EPACS operator who has permission to view that site.

Except for Site 1, we performed tests to determine whether alarms are generated when a door is opened too long, when an invalid Personal Identification Number is used, and when a SmartID card is used to enter an area where the card holder is not authorized to enter.[13] We identified one instance at Site 6 where we held the door open longer than allowed but the Door Open Too Long alarm did not appear on the EPACS Event Viewer. The local Physical Security Specialist stated that the door could be misaligned and would require a repair order from facilities management to address the issue. Once the door is repaired the door alarms should appear on the EPACS Event Viewer.

Some IRS facilities have command centers where guards monitor the EPACS Event Viewer 24 hours a day every day. We visited two such facilities. Site 1 is one of the two facilities. The other facility is one that was not included in our original selection of eight locations. The guards at this site monitor seven campus buildings within its local area including Site 3. However, no one constantly monitors the EPACS Event Viewer for the other six locations we visited. The IRM states that the IRS shall monitor physical access to the facility where the system resides to detect and respond to physical security incidents.[14] However, there appears to be no policy on who will timely address actionable alarms as they occur. Without and adequate and timely response to alarms, the IRS increases the risk of unauthorized individuals gaining access to information technology assets and sensitive taxpayer information.

The Chief, FMSS, should:

Recommendation 5: Determine the cause for the inoperable alarm at Site 6 and resolve the issue to enable alarms to appear in the EPACS Event Viewer.

Management's Response: The IRS agreed with this recommendation. The inoperable alarm identified as a "Door Open Too Long" event did not display in Velocity due to

[13] For various reasons, this was not tested at Sites 1, 2, 3, and 5.

[14] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (Dec. 13, 2022).

internal updating of information. Once the downloading finished, the system operated normally. The reader did deny and grant access as intended.

Office of Audit Comment: While the IRS agreed with the recommendation, the response does not indicate that the Door Open Too Long alarm correctly displayed in the EPACS Event Viewer after the internal update.

Recommendation 6: Establish a process to monitor the EPACS Event Viewer and timely resolve actionable alarms at all facilities with EPACS implemented, as required.

Management's Response: The IRS agreed with this recommendation. FMSS will develop and implement a process to monitor the EPACS Event Viewer and timely resolve actionable alarms at all facilities with EPACS implemented, as required.

Limited area signage and register were not always present

- Signage for the Limited Areas.
  - Two of the locations we visited had buildings that included the servers that host the EPACS. One of the buildings was Site 1 and as Figure 4 noted we did not review signage during the planning phase. The other building was subsequently included in our review because it has EPACS servers and is in a city where we already had plans to visit.[15] This latter building posted the required Limited Area signage.
  - Three sites (Sites 2, 5, and 6) had the required Limited Area signage.
  - Four sites (Sites 3, 4, 7, and 8) did not always post the required signs.

The IRM requires that Limited Area signs are prominently posted.[16] We concluded that the missing signs were due to insufficient oversight. These signs add a layer of deterrence. Without them, unauthorized personnel who attempt to enter a Limited Area could claim they were unaware that the area was only accessible to authorized individuals.

Management Action: During our visit to Site 8, the Security Section Chief took corrective action by providing Limited Area signs for the Physical Security Specialist to post.

- Form 5421, *Limited Area Register* (a form visitors are required to sign when they visit a Limited Area).
  - Two sites (Site 1 and the additional subsequent site) that included the EPACS servers posted Form 5421 and provided documentation showing that visitors obtained approval prior to entering the Limited Areas.
  - Three other sites (Sites 2, 5, and 7) had Forms 5421 posted in the Limited Areas we visited.
  - Four sites (Sites 3, 4, 6, and 8) did not have the Form 5421 in two or more of its Limited Areas.

[15] Because this subsequent site had not completed the EPACS installation, we reviewed it only for two-factor authentication requirement implementation, signage, Limited Area Register, and the required "R" designation on the SmartID card.

[16] IRM 10.2.14, *Methods of Providing Protection* (May 6, 2020).

The Information Technology organization has guidelines and standard procedures for controlling physical access to all computer rooms Service-wide.[17] An Information Technology official must approve requests for computer room access. All visitors will need a local Point of Contact and will have to be logged in, accounted for, and escorted continually while in the Limited Area. In addition, visitors, and those with escort only access must sign Form 5421, which is required to be present in Limited Areas. We concluded that the missing Forms 5421 were due to insufficient oversight. FMSS personnel stated that the Information Technology organization is responsible for posting the Forms 5421. Without a Form 5421 that is completed with the required information, management is unable to quickly identify visitors to the Limited Areas when needed.

Management Action: At the time of our testing, for Limited Areas, the IRM required signs to be posted and Forms 5421 to be completed. ACM management stated that the IRM was revised to change the areas we reviewed from Limited to Controlled; therefore, Form 5421 and the Limited signs are no longer required in the areas we visited.[18] The current IRM states that the IRS Computer Rooms in certain locations are designated Limited Areas.

Personnel with access to Limited Areas did not always have the required designation on their SmartID card

At three sites, some of the Physical Security Specialists we met did not have the "R" designation on their SmartID card but were able to unlock doors to the Limited Areas. The Physical Security Specialists at the remaining five sites and the Information Technology Specialist at the subsequent additional site had the "R" on their badge. Managers are responsible for ensuring authorized employees are issued the appropriate identification cards. The IRM states that all personnel assigned to Limited Areas must always wear a SmartID card containing the "R" indicator.[19] To be issued a SmartID card with the "R" indicator, Form 13716, *Request for ID Media for IRS Employees*, must be completed, including the "Limited Area Authorization" section, and signed by the manager of the Limited Area. The Physical Security Specialist at Site 5 was not aware of this requirement. A Physical Security Specialist at Site 6 stated that they thought the "R" was no longer required. It is unknown why the Physical Security Specialist at Site 8 did not have the indicator. The risk that unauthorized individuals in Limited Areas are not identified may increase if the "R" designation requirement on the SmartID is not enforced.

Management Action: At the time of our testing for Limited Areas, the IRM required personnel to have the "R" designation on their SmartID card.[20] ACM management stated that the IRM was revised to change the areas we reviewed from Limited to Controlled.[21] Therefore, the Physical Security Specialists are no longer required to have the "R" designation for the areas we reviewed.

[17] *IRS Enterprise Operations Computer Room Access, Standard Operating Procedures* (Dec. 2021).

[18] IRM 10.2.14, *Physical Security Program, Methods of Providing Protection* (Jan. 10, 2023).

[19] IRM 10.2.18, *Physical Access Control* (Feb. 3, 2023).

[20] IRM 10.2.18, *Physical Access Control* (Jul. 5, 2018).

[21] IRM 10.2.14, *Physical Security Program, Methods of Providing Protection* (Jan. 10, 2023).

Data in the Door Group Design Document and the EPACS did not always align

ACM management stated that an initial design document is created after installation plans are verified, provided to the ACM team, and updated during installation. It is the foundation for the door groups in the EPACS. The design document contains a description of each controller, door (including the NIST Classification, *i.e.*, Controlled or Limited Area), and card reader type among other items for each site. During our site visits, we identified 22 instances of errors in the design document or the EPACS at five of eight sites (Sites 1, 3, 4, 7, and 8) visited. Specifically,

- In 10 instances at four sites (Sites 1, 3, 4, and 8), the card reader types listed in the design document did not reflect the card readers that were installed.

  Management Action: For Site 4 only, we received documentation that confirmed the error was corrected for one of the two Site 4 instances.

- In two instances at two sites, the card reader type was incorrect and the NIST Classification was not consistently reported within the design document (Site 1) or was incorrect (Site 4).

  Management Action: We observed a contractor correcting the error in the EPACS only for Site 4's instance.

- In one instance at one site (Site 1), the NIST classification within the design document was inconsistent.

- In three instances at two sites (Sites 3 and 8), the NIST Classification, card reader type, and door name in the design document were incorrect.

  Management Action: At both sites, we observed a contractor correcting the errors in the EPACS for the three instances.

- In two instances at one site (Site 3), the door names in the design document were incorrect.

- In one instance at one site (Site 7), a door name in the design document was correct but differed from the door name in the EPACS.

  Management Action: At Site 7, we observed the ACM team determine that the EPACS had the incorrect door name and corrected the error.

- In three instances at one site (Site 3), the card reader type and door name in the design document were incorrect.

The IRM requires that to ensure the integrity of data, accurate and complete asset records are to be maintained.[22] ACM management stated that errors on the design document may have occurred due to clerical error and confirmed there is no process to verify the information during the Site Acceptance Testing done at project completion. ACM management stated that inaccuracies may require additional testing, reconfiguration, and/or updating the design document to reflect actual installation.

[22] IRM 2.149.1, *Asset Management Policy* (Sept. 29, 2022).

Recommendation 7: The Chief, FMSS, should implement a process to ensure that the design document and the EPACS have correct information and are updated when changes occur or when Site Acceptance Testing is performed.

> **Management's Response:** The IRS agreed with this recommendation. FMSS will develop and implement a process to ensure that the design document and the EPACS have correct information and are updated when changes occur or when Site Acceptance Testing is performed.

The IRS Addressed Prior Audit Recommendations to Ensure a Computer Room Is Secured With a Multi-Factor Authentication Card Reader

In a prior audit, we found that an Integrated Submission and Remittance Processing domain controller was in an unlocked room with submission processing equipment.[23] The room was accessible by personnel who did not need access to the server. We recommended that the server be physically separated from the submission processing equipment and that computer rooms be made compliant with Federal multi-factor authentication requirements. During our site visit to this location, we determined that the IRS implemented both recommendations. The server is secured in its own room and the door to the room is equipped with a Federally compliant multi-factor card reader that is configured for two-factor authentication.

[23] Treasury Inspector General for Tax Administration, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020).

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this review were to evaluate the deployment of the EPACS and security controls over the system. To accomplish our objectives, we:

- Evaluated the adequacy of the planning for the EPACS installations by interviewing FMSS personnel and analyzing the EPACS installation planning documentation that included steps to be completed at each site.
- Determined whether the IRS has effective logical access controls in place to prevent unauthorized access to the EPACS by selecting and reviewing a judgmental sample of 81 (35 active, 31 disabled, and 15 inactive for 120 days) EPACS operator accounts to verify whether the granting and disabling of account access was accomplished properly.[1] We selected the sample from a list of 1,568 EPACS operator accounts containing 766 active, 744 disabled, and 58 disabled due to 120 days of inactivity.
- Determined whether the IRS has the appropriate physical security controls in place to protect Controlled and Limited Areas by performing walkthroughs of IRS facilities and evaluating whether the IRS: 1) installed the correct card readers and programmed them as required; 2) maintained visitor access logs; 3) approved visitor requests to enter Limited Areas; 4) posted Limited Area signage as required; 5) confirmed personnel with unescorted access to Limited Areas always wore a SmartID card containing the "R" indicator; and 6) reconciled the design document and EPACS to what we observed. To perform these tests, we judgmentally selected eight sites out of a population of 75 sites that completed the EPACS installation as of July 2022. Further, we judgmentally selected and reviewed 171 doors from a population of 584 doors at the eight sites to test. We used judgmental sampling because we will not be projecting the results over the population.
- Determined whether the IRS addressed prior audit recommendations in Treasury Inspector General for Tax Administration, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020), by conducting a walkthrough to verify that the domain controller is physically separated in its own limited area and the door to the room is secured with a two-factor authentication card reader.

Performance of This Review

This review was performed at IRS offices in Atlanta, Georgia; St. Louis, Missouri; Bronx and Westbury, New York; Memphis, Tennessee; Houston, Texas; and Ogden and Salt Lake City, Utah, during the period June 2022 through June 2023. We also worked with IRS personnel from the FMSS organization, and the Information Technology organization located at the sites visited and in Washington, D.C.

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

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Khafil-Deen Shonekan, Audit Manager; Jamillah Hughes, Lead Auditor; and Tina Wong, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the BEARS. We evaluated the data by 1) reviewing existing information about the data and the system that produced them, and 2) reviewing the data for completeness. 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: NIST requirements for security of Federal information systems, EPACS Physical Security Operations Guide for logical controls and IRM 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

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 1,286 two-factor authentication card readers securing all areas within IRS facilities that are not compliant with the Federal requirements (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

During our walkthrough of Site 2, we tested nine of 24 Limited Area doors for which the design document stated that two-factor authentication card readers were installed. We determined that the two-factor authentication card readers were installed but were configured for single-factor authentication only. A Physical Security Specialist stated that all two-factor authentication card readers were configured for single-factor authentication only and were not compliant with updated Federal requirements. ACM management subsequently stated that there are an additional 1,262 of the same type of noncompliant card readers at other locations. In total, 1,286 (24 + 1,262) two-factor authentication card readers securing all areas within IRS facilities are not compliant with the current Federal standards.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF
FACILITIES MANAGEMENT AND
SECURITY SERVICES

September 5, 2023

MEMORANDUM FOR HEATHER M. HILL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard L. Rodriguez
Chief, Facilities Management & Security Services

Digitally signed by Richard L. Rodriguez
Date: 2023.09.05 09:52:12 -04'00'

SUBJECT: Draft Audit Report – The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement (Audit # 202220023)

Thank you for the opportunity to review and comment on the draft audit report. We appreciate that your report acknowledged that the methodology used to select and prioritize IRS facilities for the EPACS installation was effective and that the planning tool used to guide the installation project from planning to completion was working as intended. You also acknowledged that the Access Control Management team follows physical access policy in compliance with all applicable Federal directives and aligns with IRS and FMSS Strategic Plans to protect employees and facilities. Your recommendations will assist us in our efforts to ensure that access to facilities and sensitive taxpayer information is timely revoked for separated employees.

With the exception of part of Recommendation 4, we agree with your recommendations and have developed corrective actions to remediate the majority of the report findings. We disagree with part of recommendation 4. Due to the update to IRM 10.2.14.3.5, the 2 Site 1 doors in question are now designated not as limited access areas but as controlled areas that require single factor authentication only.

We have already begun making progress on Recommendations 1, 3 and 7. For example, for Recommendation 1, FMSS is in the process of developing and deploying a Velocity Operator Guide and partnering with Cybersecurity to update and clarify the BEARS entitlement and EPACS roles request process. For Recommendation 3, FMSS revised IRM 10.2.14.3.5 to redesignate Main Distribution Frame /Intermediate Distribution Frame rooms not as limited access but as controlled space and reduced the number of noncompliant card readers. For Recommendation 7, FMSS has started testing a new process for verifying and updating design documents during Site Acceptance Testing.

We concur with the described value of outcome measure. 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) 317-4480, or a member of your staff may contact Brian Soloman, Associate Director, Security, Facilities Management and Security Services at (231) 493-8977.

Attachment

Attachment

Recommendation #1:
The Chief, FMSS, should update the EPACS Operations Guide to provide clarity on granting and disabling operator accounts and the specific entitlements that are required in the BEARS for all EPACS roles.

CORRECTIVE ACTION:
We agree with this recommendation. FMSS will develop and implement a new Velocity Operator Guide that will provide clarity on granting and disabling operator accounts and the specific entitlements that are required in the BEARS for all EPACS roles.

IMPLEMENTATION DATE:
September 15, 2024

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #2:
The Chief Information Officer should ensure that the Cybersecurity function's Enterprise Security Audit Trails team in collaboration with the ACM team prioritizes completing the Audit Worksheet so that the audit logs can be monitored and reviewed.

CORRECTIVE ACTION:
We agree with this recommendation. The Chief Information Officer in close partnership with FMSS will complete the Audit Worksheet to enable the audit logs to be monitored and reviewed.

IMPLEMENTATION DATE:
November 15, 2024

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer, Cybersecurity

RECOMMENDATION #3:
The Chief FMSS should ensure that all 1,286 noncompliant card readers are replaced with Federally compliant card readers and are properly configured.

CORRECTIVE ACTION:
We agree with this recommendation. FMSS will ensure that all noncompliant card readers are replaced with Federally compliant card readers and are properly configured.

IMPLEMENTATION DATE:
September 15, 2025

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #4:
The Chief FMSS should replace the two single-factor authentication card readers in the Limited Areas at Site 1 and the broken two-factor authentication card reader at Site 3.

CORRECTIVE ACTION #1:
Site 1- We disagree with this recommendation. The areas are not limited access areas and do not require two-factor readers.

IMPLEMENTATION DATE:
N/A

CORRECTIVE ACTION #2:
Site 3 – We agree with this recommendation and consider it complete. At the time the two-factor reader stopped working, it was under warranty. The Vendor was on site on October 25, 2022, and replaced the broken two-factor reader with a working two-factor reader.

IMPLEMENTATION DATE:
Implemented October 25, 2022

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #5:
The Chief FMSS should determine the cause for the inoperable alarm at Site 6 and resolve the issue to enable alarms to appear in the EPACS Event Viewer.

CORRECTIVE ACTION:
We agree with this recommendation and consider it complete. The inoperable alarm, identified as a 'Door Open Too Long' event, did not display in Velocity due to internal updating of information. Once the downloading finished, the system operated normally. The reader did deny, and grant access as intended.

IMPLEMENTATION DATE:
November 16, 2022

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #6:
The Chief FMSS should establish a process to monitor the EPACS Event Viewer and timely resolve actionable alarms at all facilities with EPACS implemented, as required.

CORRECTIVE ACTION:
We agree with this recommendation. FMSS will develop and implement a process to monitor the EPACS Event Viewer and timely resolve actionable alarms at all facilities with EPACS implemented, as required.

IMPLEMENTATION DATE:
September 15, 2024

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #7:
The Chief, FMSS, should implement a process to ensure that the design document and the EPACS have correct information and are updated when changes occur or when Site Acceptance Testing is performed.

CORRECTIVE ACTION:
We agree with this recommendation. FMSS will develop and implement a process to ensure that the design document and the EPACS have correct information and are updated when changes occur or when Site Acceptance Testing is performed.

IMPLEMENTATION DATE:
September 15, 2024

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

Appendix IV

Glossary of Terms

Term	Definition
Active Directory	An application that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. Active Directory also enables administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization simultaneously from a central, organized, accessible database.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Business Entitlement Access Request System	Manages the identity access management for all of the IRS.
Controlled Area	A security area which requires one single authentication mechanism to ensure that only authorized personnel have unescorted access.
Domain Controller	A server that is running a version of the operating system and has Active Directory Domain Services installed.
Enterprise Physical Access Control System Event Viewer	Displays events involving doors, *e.g.*, access granted, and door open too long.
Entitlement	Rights granted to the user of licensed software that are defined within the license agreement.
Limited Area	A security area to which access is limited to authorized personnel by a two-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.
Receipt and Control	An area that receives all mail addressed to the IRS and delivered by the U.S. Postal Service.
Role-Based	Access control based on user roles, *i.e.*, a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role. Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization.

Term	Definition
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 V

Abbreviations

ACM	Access Control Management
BEARS	Business Entitlement Access Request System
EPACS	Enterprise Physical Access Control System
FMSS	Facilities Management and Security Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

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