TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

More Controls Could Help Prevent Unauthorized Access to Taxpayer Information

August 12, 2026

Report Number: 2026-IE-R013

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

HIGHLIGHTS: More Controls Could Help Prevent Unauthorized Access to Taxpayer Information

Final Evaluation Report issued on August 12, 2026 Report Number 2026-IE-R013

Why TIGTA Did This Evaluation

In 2023, an IRS contractor admitted to accessing a database to collect tax return information on thousands of the nation's wealthiest individuals.

In 2024, we reported on how the IRS grants access to, and safeguards federal tax information maintained on its various information technology systems.

This evaluation was a follow-up review to assess whether the IRS has taken appropriate actions to ensure that only authorized employees and contractors have access to the IRS network and sensitive systems.

Impact on Tax Administration

Unauthorized access can lead to disclosure of taxpayer information, which undermines public trust in the IRS's ability to safeguard confidential tax information. It is essential that users without a business reason, such as those on administrative leave, do not retain access to the IRS's network or sensitive systems.

What TIGTA Found

The IRS manages access to its various systems through the Business Entitlement Access Request System (BEARS). We identified that almost 17,000 of the nearly 21,500 employees who took one of the deferred resignation programs retained access to the IRS network while on administrative leave as of June 2025. Further, approximately 14,000 of the nearly 21,500 employees still had access to one or more sensitive systems.

To safeguard federal tax data, the IRS must ensure that users with access to the IRS network and sensitive systems are removed when they separate from the IRS. We also found that some employees who took a deferred resignation offer could have accessed IRS facilities or systems because the IRS did not initially have a policy to collect or disable the Personal Identity Verification (PIV) cards of employees on administrative leave. However, the IRS began working with the Treasury Department to disable computer access for PIV cards of employees who took the deferred resignation.

Additionally, over 550 of the nearly 1,200 employees and contractors hired between January and August 2025 did not complete appropriate security awareness training prior to gaining sensitive systems access.

What TIGTA Recommended

We made six recommendations to the Chief, Information Officer.

Our recommendations included:

- Identify all employees who accepted a deferred resignation program offer and are on administrative leave. Revoke the access of these employees to IRS sensitive systems and the IRS network in BEARS.
- List the specific training course requirements for systems access in the Internal Revenue Manual.
- Implement a process to ensure that employees and contractors are not granted access to any sensitive systems without completing required security training.

The IRS agreed with five recommendations and partially agreed with one recommendation.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: August 12, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Nancy A. LaManna
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – More Controls Could Help Prevent Unauthorized Access to Taxpayer Information (Evaluation No.: IE-25-032)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has taken appropriate corrective actions to ensure users are properly vetted before gaining access to sensitive systems and that sensitive system access is timely removed for all users who separate from the IRS. Members of the United States Senate also requested that we investigate reports of improper access to tax return information. This review is part of our Fiscal Year 2026 Annual Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

Management's complete response to the draft report is included as Appendix II. If you have any questions, please contact me or Frank O'Connor, Director, Inspections and Evaluations.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 2

Some Employees Who Took a Deferred Resignation Retained Access to Sensitive Systems ..... Page 2

Recommendation 1: ..... Page 3

Recommendations 2 through 4: ..... Page 6

Training Requirements Are Not Specific and Not Always Completed Prior to Gaining Sensitive Systems Access ..... Page 6

Recommendations 5 and 6: ..... Page 8

Employee and Contractor Background Investigations Are Being Conducted as Required ..... Page 9

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 10

Appendix II – Management's Response to the Draft Report ..... Page 11

Appendix III – Abbreviations ..... Page 15

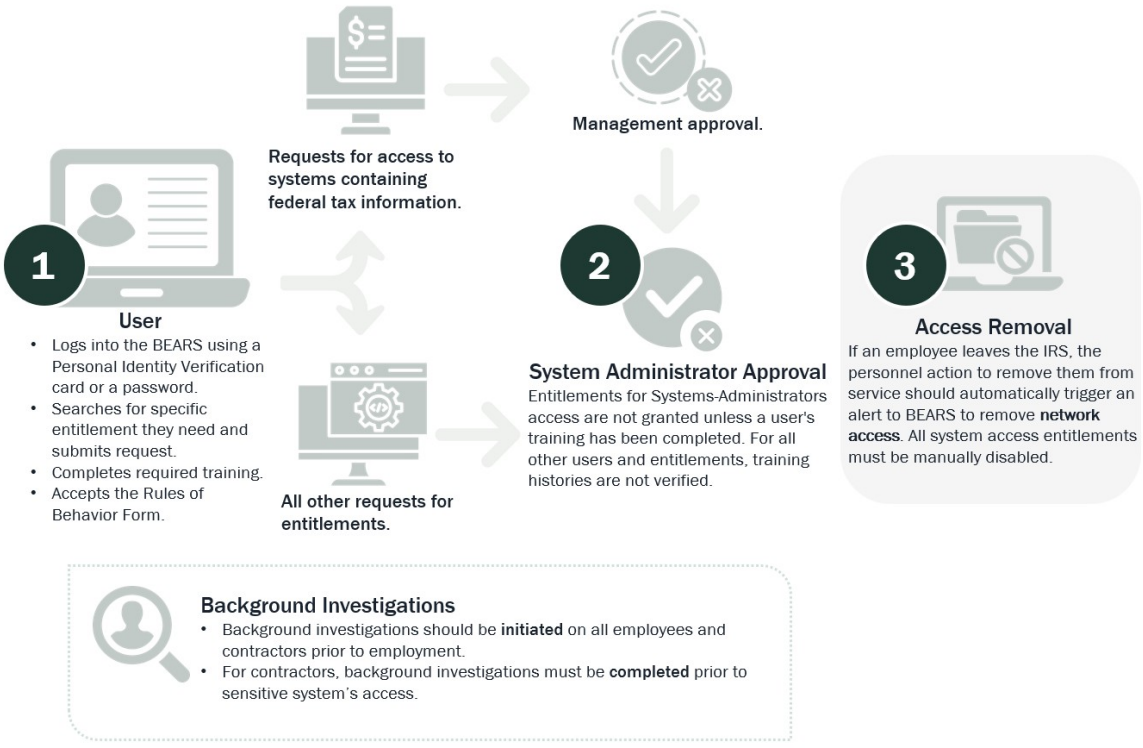
Background

In 2024, we reported on how the Internal Revenue Service (IRS) grants access to and safeguards federal tax information maintained on its various information technology systems.[1] The evaluation was performed after an IRS contractor accessed a database to collect tax return information on a high-ranking government official and thousands of the nation's wealthiest individuals. The data were uploaded to a private website to avoid detection and then shared with media organizations. The former contractor was later sentenced to five years in prison.

In that evaluation, we reported that procedures to systemically remove users who no longer required access to sensitive systems were not always working as intended. We also identified that the IRS did not always remove contractor access to sensitive systems when background investigations were not favorable.

The IRS manages access to its various systems through the Business Entitlement Access Request System (BEARS). The BEARS system itself does not collect any taxpayer, or other sensitive information, and not all information systems managed in BEARS contain sensitive data. The IRS requires first-level managers to approve requests to access systems containing federal tax information. For all other access requests, a system administrator will decide whether to grant access. Figure 1 summarizes the BEARS entitlement process.

Figure 1: Overview of the BEARS Entitlement Process



Source: TIGTA analysis of the BEARS process.

[1] TIGTA, Report No. 2024-IE-R008, *Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information* (February 2024).

In January 2025, the IRS began reducing the overall size of its workforce through the Deferred Resignation Program (DRP) and the Treasury Deferred Resignation Program. These programs allowed employees to voluntarily resign and generally be placed on administrative leave until September 30, 2025. In July 2025, we reported that 21,646 employees had taken a deferred resignation.[2] Since these employees were on administrative leave, they no longer had a business reason for retaining access to the IRS's network or sensitive systems. Unauthorized access can lead to disclosure of taxpayer information, which undermines public trust in the IRS's ability to safeguard confidential tax information.

We initiated this evaluation to assess whether the IRS had taken appropriate steps to ensure that only authorized employees and contractors retained access to IRS systems. Also, in April 2025, we received a congressional request to review whether anyone had improperly accessed tax return information.

Results of Review

Our review found that approximately 17,000 of the nearly 21,500 employees on administrative leave due to the deferred resignation programs retained access to the IRS network. Additionally, over 14,000 of the nearly 21,500 employees kept access to one or more sensitive systems. These employees did not have a legitimate business reason to retain this access and posed a potential security risk for unauthorized disclosure of sensitive information. Further, some of these individuals could have accessed IRS facilities or systems because the IRS did not initially have a policy to collect or disable Personal Identity Verification (PIV) cards of employees on administrative leave.

Additionally, of the nearly 1,200 employees and contractors hired since January 2025, we identified more than 550 users who did not complete the required security training prior to receiving systems access.

We also learned that some IRS and non-IRS users were granted access to at least one system outside the BEARS entitlement process in violation of IRS policy. TIGTA's Office of Audit is currently assessing the extent that users were granted access to any systems outside the BEARS process and the potential impacts and will issue a separate audit report.

Some Employees Who Took a Deferred Resignation Retained Access to Sensitive Systems

The IRS did not have an effective process to timely remove system access for employees who are placed on administrative leave. The IRS provided a listing of nearly 21,500 employees who accepted a deferred resignation as of May 2025. We assessed whether the employees retained access to the IRS network or a sensitive system in BEARS. Our review found that as of June 2025, nearly 17,000 of the 21,500 employees retained access to the IRS network and over 14,000 employees had access to systems with sensitive taxpayer information. Since these employees were placed on administrative leave, they did not have a business reason to retain this access.

[2] TIGTA, Report No. 2025-IE-R027, *Snapshot Report: IRS Workforce Reductions as of May 2025* (July 18, 2025).

In June 2025, we alerted the IRS that the employees who took a deferred resignation still had network and sensitive system access and that there was a risk of unauthorized access and disclosure. We recommended that the IRS remove access to the network and sensitive systems for the identified employees. During our previous review, the IRS stated that the risks posed by employees retaining access to sensitive systems were reduced but not eliminated because their network access should be systematically removed when they separate. Without network access, the employee should not be able to access any sensitive systems. However, some of the separated users in our current review have a higher risk than the users identified in our 2024 review because the users retained both sensitive systems entitlements and the IRS network necessary to access them.

The IRS indicated that it was working to manually remove the access of these employees.

Generally, when a user's employment status changes, the human resources system generates a personnel action request, which is automatically sent to BEARS. For example, if someone separates from the IRS (*e.g.*, an employee retires, leaves, or is suspended or terminated), BEARS will automatically revoke the employee's access to the IRS network. However, according to IRS officials, employees who accepted a deferred resignation still had their system entitlements because they had not officially separated from the IRS. When the employees were placed on administrative leave and did not officially separate, a personnel action request was not created to deactivate network or systems access in BEARS.

Ensuring that users with access to the IRS network and sensitive systems are timely removed when they separate from the IRS is essential to safeguarding federal tax data.

Recommendation 1 (Email Alert): The Chief, Information Officer, should coordinate with the Human Capital Office (HCO) to identify all employees who accepted a deferred resignation and are on administrative leave and revoke their access to IRS sensitive systems and the IRS network in BEARS.

> **Management's Response to Email Alert:** The IRS agreed and confirmed that employees who accepted both versions of the DRP still have active entitlements since their official separation has not yet occurred. IRS Information Technology has been working closely with the HCO to validate employees who accepted the deferred resignation. Entitlements will be removed as employees are validated and confirmed to be on administrative leave or have separated.

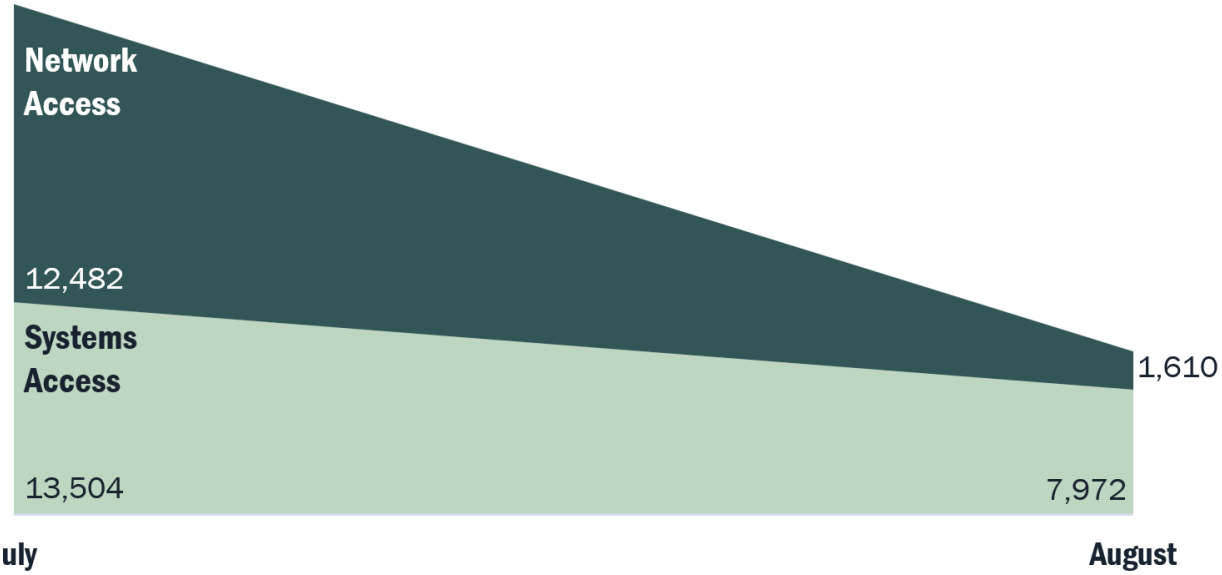
We continued to monitor the IRS's corrective actions to confirm whether entitlements were removed for employees that accepted the deferred resignation and were on administrative leave.

The IRS made progress removing some employees' systems access

Following our recommendation, the IRS began removing access from employees that took a deferred resignation. As of July 2025, about 13,500 employees retained systems access, and about 12,500 retained access to the IRS network. By August 2025, the number had decreased to below 8,000 with sensitive systems access and about 1,600 with IRS network access. While we acknowledge the IRS took swift action, they still must implement a process to immediately terminate system access when a business need to access taxpayer information no longer exists.

Figure 2 shows the number of users that retained systems and network entitlement access between July and August 2025.

Figure 2: Decrease in DRP Employees' System and Network Access From July to August 2025



Source: TIGTA analysis of BEARS user data and IRS employee DRP data, as of July and August 2025. IRS employee DRP data, as of May 2025, are also included.

Concerns remain with separated employees having sensitive systems and network access

As of August 2025, we identified individuals who separated from the IRS and retained active access to the IRS network and sensitive systems. Our review found 46 individuals who did not take a deferred resignation but separated and retained active network access. Of these, nine also had active access to a sensitive system.

In our 2024 report, we recommended that the IRS ensure that network and sensitive system access are timely removed for users who separate from the IRS. The IRS agreed with the recommendation, confirmed that system-level user accounts would be removed, and started plans to enhance its procedures for identifying and resolving separate user accounts that have not been promptly removed.

At the time, the corrective action was based on the IRS's personnel tracking system being systemically integrated with BEARS. When the employment status changed, the system sent information to BEARS, which automatically removed the user's network access. However, this process was not designed to remove system entitlements. Further, the process did not apply to employees who essentially separated from the IRS but remained in an active status in the personnel system due to being on administrative leave.

Some employees' network access is still not documented in the Business Entitlement Access Request System

Separately, we identified 107 users in IRS Criminal Investigation (IRS-CI), the agency's law enforcement branch, that had access to sensitive systems but with no network access

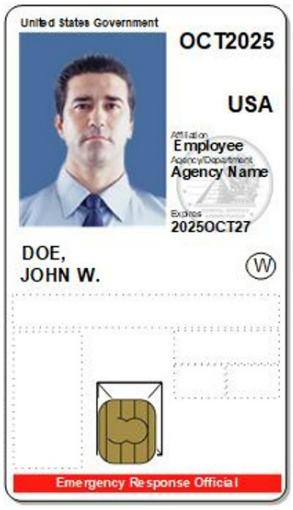
documented in BEARS. However, we confirmed that these users do in fact have network access. In our prior report, we identified more than 1,500 IRS-CI users with access to a sensitive system that did not have network access documented in BEARS.

These users were the first to migrate to BEARS prior to the IRS establishing a network access approval process. Therefore, network access was not documented for some users' accounts and were not updated when the IRS converted to BEARS from the previous access control system. The IRS agreed with our recommendation to update the network access for these employees and closed out the recommendation as completed.

Per the IRS, this recommendation has been fully implemented, however, our current finding indicates these actions did not fully correct the issue.

No initial process in place to collect Personal Identity Verification cards used for systems access by Deferred Resignation Program employees

The IRS did not initially have a process in place to collect PIV cards of DRP employees. PIV cards are federal government-issued identification cards that allow access to secure facilities and are used to access information systems and networks. These cards are highly resistant to identity fraud, tampering, counterfeiting, and exploitation. PIV cards can be used for:



Source: GSA.gov.

- Privileged access to servers, networks, and applications and systems.
- Authentication on sensitive networks and applications.
- Access to facilities.

Generally, managers and Contractor Representatives have the responsibility to:

- Recover PIV cards of employees and contractors who separate or are placed in a nonwork status on their last workday and send them to the local Facilities Management and Security Services (FMSS) Security office for disposition or retention.
- Report unrecovered PIV cards.
- Certify the disposition of PIV cards.

FMSS is responsible for terminating PIV cards when IRS employees and contractors leave the agency. The FMSS must collect PIV cards when:

- An employee receives a replacement PIV card.
- A PIV card designation is no longer valid.
- An employee separates (termination, resignation, retirement, or transferring to another federal agency).
- An employee is placed on a nonwork status.

Employees who accepted the deferred resignation did not get an identifier in the human resources system and were designated as "active." As a result, the normal separating employee

clearance process was not followed. According to the IRS, beginning in February 2025, the IRS provided supplemental guidance to employees and managers detailing requirements to follow when going on administrative leave. The IRS explained that given the speed that employees were placed on administrative leave and the fact that employees and managers were often not co-located, collecting PIVs was difficult. According to FMSS officials, the IRS initiated an *ad hoc* separation process that used DRP participant lists to disable the PIV card from being used to access buildings. In addition, the IRS provided DRP rosters to their counterparts at the Department of the Treasury who terminated the PIV card's certificates so they could not access information systems. In the event of additional deferred resignation offerings, the IRS should establish procedures to ensure PIV cards are collected.

The Chief, FMSS, should:

Recommendation 2: Establish procedures to ensure that PIV cards are recovered from employees who participate in future DRPs or otherwise placed on administrative leave.

> **Management's Response:** The IRS agrees with this recommendation. FMSS will publish procedures to require that PIV cards are recovered from employees who participate in future DRPs or are otherwise placed on administrative leave that is expected to end in separation.

The Chief, Information Officer, should:

Recommendation 3: As previously recommended, ensure that all user network access and sensitive system access are immediately removed for users who separate from the IRS. Also ensure that controls are in place to prevent employees from retaining access in the future.

> **Management's Response:** The IRS agrees with this recommendation. According to the IRS, the Chief Information Officer fully implemented the automated removal of user network access for employees and contractors recorded as separated in the IRS personnel system and has controls in place to prevent employees from retaining access in the future.

The Chief, Criminal Investigation, should:

Recommendation 4: Ensure that all IRS-CI users have updated network access records in BEARS.

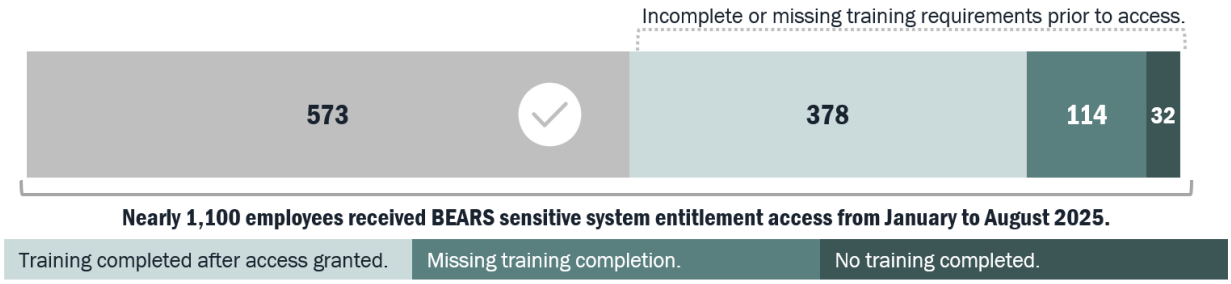
> **Management's Response:** The IRS agrees with this recommendation. The Chief, Criminal Investigation, will ensure that all the IRS-CI users have updated and accurate network access records documented in the BEARS.

Training Requirements Are Not Specific and Not Always Completed Prior to Gaining Sensitive Systems Access

Between January and August 2025, nearly 1,100 new employees received a BEARS sensitive system entitlement. Of these new employees, we identified 524 employees who either completed cybersecurity training after their entitlement approval date or did not complete all training modules. Specifically, 378 employees completed training after they were granted systems access. Further, 114 employees were granted access, but they did not complete all

training courses at the time of our analysis, and 32 of these employees did not take any of the courses.

Figure 3: New IRS Employee Training Completion Before Systems Access



Source: TIGTA analysis of IRS Employee Training Histories and BEARS Entitlement Records.

The Internal Revenue Manual (IRM) does not have a specific list of required training courses that employees and contractors must complete before accessing sensitive systems. The IRM is the primary, official compilation of instructions to staff that relate to the administration and operation of the IRS. The IRM broadly states some training topics that must be completed before users are given access to sensitive information. For example, it mentions IRS annual and role-based privacy, information protection, and disclosure training requirements, unauthorized access awareness briefings, and records management briefings.

Although the employee is responsible for completing the required training, the IRS does have a systematic process to block users from being approved for certain systems. The BEARS will not approve systems-administrator access if the user has not completed required training.[3] However, this process does not apply to most systems that employees and contractors can get access to use.

In 2023, the Government Accountability Office (GAO) identified several IRS training courses that relate to protecting taxpayer information.[4] We reviewed employee and contractor training using the courses identified by GAO. Figure 4 lists four courses that the GAO identified for IRS employees and five courses for IRS contractors.

[3] A Systems Administrator manages, configures, and maintains an organization's IT infrastructure and generally has elevated, higher risk access rights.

[4] Government Accountability Office, GAO-23-105395, *Security of Taxpayer Information* p. #67-68 (August 2023).

Figure 4: GAO Identified Employee and Contractor Cybersecurity Training Requirements

Name of Training	IRS Employee	IRS Contractor
IRS Annual Cybersecurity Awareness Training	☑	☑
Insider Threat Awareness	☑	☑
Privacy, Information Protection & Disclosure	☑	☑
Unauthorized Access, Attempted Access, or Inspection of Tax Records (UNAX) Awareness	☑	☒
Introduction to UNAX	☒	☑
Inadvertent Sensitive Information Access	☒	☑

Source: TIGTA analysis of training courses and requirements identified by GAO.

Contractors given systems access before completing training

We found that 91 new contractors requested their earliest system entitlement in BEARS between January and August 2025. Furthermore, of the 91 contractors, we identified:

- 12 had not taken any of the 5 GAO identified courses.
- 8 had not taken any training course.
- 7 either did not have a recorded training history or could not be found in the IRS web-based learning module.

According to the IRS Acquisition Policy, all contractors requiring staff-like access to sensitive information, including taxpayer information, must complete IRS-provided privacy and security awareness training, including *Privacy, Information Protection & Disclosure* training. Contractors should not access taxpayer information without completing all training. However, based on the contractors we identified above, there does not appear to be a process to prevent or remove systems access for contractors with incomplete training requirements.

The HCO should:

Recommendation 5: List the specific training course requirements for systems access in the IRM.

> **Management's Response:** The IRS partially agrees with this recommendation. The HCO will list the specific training course requirements for systems access on the Mandatory Briefings SharePoint site and update the IRM with a link to this site. To prevent the administrative burden of frequent IRM updates, the Mandatory Briefings SharePoint site will serve as the authoritative source for current training requirements and be updated if changes are made to the required training.

Recommendation 6: Review the training histories of the employees and contractors TIGTA identified and work with the Office of Information Technology to ensure that access is removed until users complete the required training. Further, implement a process to ensure that

employees and contractors are not granted access to any sensitive systems before completing required security training.

Management's Response: The IRS agrees with this recommendation. The IRS will verify training completion for the employees and contractors identified by TIGTA, remove system access as warranted, and ensure that access to sensitive systems is granted only after required security training has been completed.

Employee and Contractor Background Investigations Are Being Conducted as Required

We reviewed our population of nearly 1,200 new users who received a BEARS sensitive system entitlement from January through August 2025. Each of these users (employees and contractors) had a required pre-employment check completed prior to being granted access to a sensitive system. While we found that full background investigations were completed for 533 employees *after* they were granted access to sensitive systems, this is allowed by IRS policy.

Background investigations verify a candidate's honesty, character, and ability to perform the job. Unsuitable candidates can expose sensitive information, and, in some cases, be a threat to national security and public safety. IRS policy states that they must initiate a background investigation into all employees and contractors prior to permitting access to federal tax information. The IRS uses prescreen-investigation dates as an interim suitability determination to allow employees to work without a complete investigation. This suitability determination is used to decide if an employee or contractor's prior conduct would or would not protect the integrity or promote the efficiency of the IRS. This prescreen-investigation includes a review of Federal Bureau of Investigations (FBI) fingerprint results, tax compliance report, and their declaration for federal employment.

Background investigations for those granted access to federal tax information must include, at a minimum, FBI fingerprinting, U.S. citizenship, and a check of local law enforcement agencies. Once an individual is onboarded as a new employee, the IRS completes the full background investigation. All background investigations should be completed within a new employee's first year of service.

We previously recommended that the IRS suspend and disable access to sensitive systems when a contractor has an unfavorable background determination. The IRS agreed with this recommendation and indicated that HCO Personnel Security Specialists will notify the Contracting Officer's Representative (COR) when this occurs. The COR then follows separation procedures and initiates actions in the personnel system to trigger the automated process to remove network access and manually disable other entitlements in BEARS. In response to our prior report's recommendations, the IRS was still developing additional training for CORs to ensure that they comply with separation procedures and timelines. Additionally, the IRS was evaluating whether to automate the access removal process, which would require integrating IRS systems with Treasury's personnel system.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has taken appropriate corrective actions to ensure users are properly vetted before gaining access to sensitive systems and that sensitive systems access is timely removed for all users who separate from the IRS. To accomplish our objective, we:

- Determined what individuals and entities have access to IRS systems containing taxpayer information (*e.g.*, IRS employees, contractors, researchers, other federal and state government agencies and employees, *etc.*). We also assessed whether users' access was revoked or denied in accordance with IRS policy.
- Determined how access and privileges to sensitive systems are granted, revoked, or otherwise managed relative to the need for continued access to sensitive information.
- Identified mandatory prerequisite training and background investigation requirements necessary to access the IRS's network and systems. We also identified employees and contractors who did not meet one or more of these requirements.
- Evaluated IRS procedures used to assure system access is revoked when users (employees and contractors) accept deferred resignations.
- Determined whether the IRS implemented corrective actions to address recommendations from our 2024 review.[1]

Performance of This Review

This review was performed with information obtained from the IRS's Human Capital and Information Technology offices located in Washington, D.C., during the period of February through December 2025. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Data Validation Methodology

We performed tests to assess the reliability of data from BEARS, the Automated Background Investigations System, and the Treasury HCO employee personnel system. We evaluated the data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

[1] TIGTA, Report No. 2024-IE-R008, *Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information* (February 2024).

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 7, 2026

MEMORANDUM FOR NANCY A. LAMANNA
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS

FROM: Kaschit Pandya
Chief Information Officer
Donald C. Drake Digitally signed by Donald C. Drake Date: 2026.07.07 14:00:45 -04'00'

SUBJECT: Draft Evaluation Report – More Controls Could Help Prevent Unauthorized Access to Taxpayer Information (Evaluation #IE-25-032)

Thank you for the opportunity to review and comment on the draft audit report. The Internal Revenue Service (IRS) takes seriously its core responsibility to safeguard federal tax information. We have significantly strengthened internal controls, protocols, and procedures related to protecting taxpayer data from unauthorized access, and many of the issues identified in this report have been addressed or are being addressed through corrective actions.

Continuous improvement remains the cornerstone of all the IRS data security programs. The IRS agrees with the audit team's recommendations, with partial agreement on Recommendation 5. For that recommendation, the IRS will address the underlying risk by taking an alternative approach that ensures we maintain an authoritative source of the current training requirements while avoiding unnecessary administrative burden. Please refer to the attachment for specific details.

The IRS appreciates the continued oversight and review provided by your office. If you have any questions, you or a member of your staff may contact Kaschit Pandya, Chief Information Officer, at 202-317-5000.

Attachment

The Internal Revenue Service (IRS) Management Response to TIGTA Draft Report
More Controls Could Help Prevent Unauthorized Access to Taxpayer Information
(IE-25-032)

Recommendations

RECOMMENDATION 1 (Email Alert): The Chief Information Officer should coordinate with the Human Capital Office (HCO) to identify all employees who accepted a DRP and are on administrative leave and revoke their access to IRS sensitive systems and the IRS network in BEARS.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. The Human Capital Office (HCO) will identify all employees who accepted the Deferred Resignation Program (DRP) and were/are on administrative leave and the Chief Information Officer (CIO) will coordinate with the HCO and revoke access to the IRS sensitive systems and the IRS network in the Business Entitlement Access Request System (BEARS).

IMPLEMENTATION DATE: August 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 2: The Chief Facilities Management and Security Services should establish procedures to ensure that PIV cards are recovered from employees who participate in future Deferred Resignation Programs or otherwise placed on administrative leave.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Facilities Management and Security Services (FMSS) will publish procedures to require that Personal Identity Verification (PIV) cards are recovered from employees who participate in future deferred resignation programs or are otherwise placed on administrative leave that is expected to end in a separation.

IMPLEMENTATION DATE: November 15, 2026

RESPONSIBLE OFFICIAL(S): Chief, Facilities Management & Security Services

RECOMMENDATION 3: The Chief Information Officer should, as previously recommended, ensure that all user network access and sensitive system access are immediately removed for users who separate from the IRS. Also ensure that controls are in place to prevent employees from retaining access in the future.

CORRECTIVE ACTION 3: The IRS agrees with the recommendation and has already implemented corrective actions. The Chief Information Officer fully implemented the automated removal of user network access for employees and contractors recorded as separated in the IRS personnel system and has controls in place to prevent employees from retaining access in the future.

IMPLEMENTATION DATE: June 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 4: The Chief Criminal Investigation should ensure that all IRS-CI users have updated network access records in BEARS.

CORRECTIVE ACTION 4: The IRS Criminal Investigation (IRS-CI) agrees with this recommendation. The Chief, Criminal Investigation, will ensure that all the IRS-CI users have updated and accurate network access records documented in the BEARS.

IMPLEMENTATION DATE: October 15, 2026

RESPONSIBLE OFFICIAL(S): Deputy Director, Technical Operations, Criminal Investigation

RECOMMENDATION 5: The Human Capital Officer should list the specific training course requirements for systems access in the IRM.

CORRECTIVE ACTION 5: The IRS partially agrees with this recommendation. The Human Capital Office will list the specific training course requirements for systems access on the Mandatory Briefings SharePoint site and update the Information Resources Management (IRM) with a link to this site. To prevent the administrative burden of frequent IRM updates, the Mandatory Briefings SharePoint site will serve as the authoritative source for current training requirements and be updated if changes are made to the required trainings.

IMPLEMENTATION DATE: January 15, 2027

RESPONSIBLE OFFICIAL(S): Director, Talent Development, Human Capital Office

RECOMMENDATION 6: The Chief Information Officer should work with the Human Capital Office to review the training histories of the employees and contractors TIGTA identified and work with the Office of Information Technology to ensure access is removed until users complete the required training. Further, implement a process to ensure that employees and contractors are not granted access to any sensitive systems before completing required security training.

CORRECTIVE ACTION 6: The IRS agrees with the recommendation. The IRS will verify training completion for the employees and contractors identified by Treasury Inspector General for Tax Administration (TIGTA), remove system access as warranted, and ensure that access to sensitive systems is granted only after required security training has been completed.

IMPLEMENTATION DATE: October 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cyber

Appendix III

Abbreviations

BEARS	Business Entitlement Access Request System
COR	Contracting Officer's Representative
DRP	Deferred Resignation Program
FBI	Federal Bureau of Investigation
FMSS	Facilities, Management and Security Services
GAO	Government Accountability Office
HCO	Human Capital Office
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IRS-CI	IRS Criminal Investigation
PIV	Personal Identity Verification
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access, Attempted Access, or Inspection of Tax Records

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 www.tigta.gov/form/suggestions.

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