

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Improvements to the IRS's Unauthorized Access Program Could Further Protect Taxpayer Privacy

September 29, 2026

Report Number: 2026-300-058

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

HIGHLIGHTS: Improvements to the IRS's Unauthorized Access Program Could Further Protect Taxpayer Privacy

Final Audit Report issued on September 29, 2026

Report Number 2026-300-058

Why TIGTA Did This Audit

The Taxpayer Browsing Protection Act made it unlawful for IRS employees to access or attempt to access taxpayer records unless there is a legitimate tax administration purpose to do so. Unauthorized access can be punished criminally and civilly.

We assessed the efficiency and effectiveness of the IRS's unauthorized access, attempted access, or inspection of taxpayer records (UNAX) program.

The mission of the UNAX program is to provide awareness to all IRS employees to ensure that they do not compromise public confidence by engaging in unauthorized access of taxpayer records. IRS employees are subject to removal per the IRS's policy and under the Taxpayer Browsing Protection Act.

The IRS is also required (per Internal Revenue Code Section 7431) to provide notices to taxpayers whose tax records were unlawfully accessed or inspected by an IRS employee.

Impact on Tax Administration

The inability to protect sensitive data may result in unauthorized access, disclosure, misuse, improper modification, or destruction of taxpayer information. This burdens affected taxpayers and violates their rights to confidentiality. Unauthorized access or disclosure can also erode public trust in the IRS, which may affect a taxpayer's decision to voluntarily comply with their tax obligations.

What TIGTA Found

The IRS's UNAX program is not adequately addressing the risk of unauthorized access to taxpayers' accounts. We found deficiencies in the following controls and/or processes intended to protect taxpayers and hold employees accountable for their actions.

Prevention: Preventative controls are primarily limited to restricted access by IRS employees to accounts of family or close relations. The IRS does not have a mechanism to prevent or systemically detect browsing of celebrities. We researched Integrated Data Retrieval System audit logs from Calendar Years 2022 through 2025 as of November 2025 and identified 86 suspicious accesses on 30 different taxpayers by 52 employees. Taxpayer records accessed included United States government officials, business leaders, and entertainers. We have referred the 86 suspicious accesses to our Office of Investigations for further action. Overall, the IRS lacks sufficient preventative controls to stop unauthorized access and has not effectively identified suspicious unauthorized accesses post access.

Discipline: The IRS's discipline process involves the application of the Douglas Factors, which are case law factors used to weigh the appropriateness of punishment for misconduct. The IRS agrees that consistently applying the Douglas Factors is imperative and that the most important factor to consider is the nature and seriousness of the offense. However, we identified 22 employees who were not terminated but had accessed taxpayer records without the taxpayer's consent or the IRS's authorization. On July 2, 2026, the Office of Personnel Management and the Merit Systems Protection Board proposed a new rule to stop applying the Douglas Factors to improve the accountability of employees for misconduct.

Victim Notification: The IRS failed to notify 175 taxpayers that their records were accessed by an unauthorized IRS employee because employees did not follow procedures. The IRS agreed that the 175 taxpayers should have been notified. An additional 101 taxpayers were not notified because the IRS only requires taxpayer notification when employee discipline is proposed. The IRS employees responsible for these unauthorized accesses either resigned or retired before disciplinary action was proposed. We also determined that the IRS does not always timely notify impacted taxpayers.

What TIGTA Recommended

We made eight recommendations to improve the UNAX program, including: study technologies to implement preventative controls; clarify guidance on the application of Douglas Factors emphasizing; and work towards a new process that ensures that all impacted taxpayers are notified of willful unauthorized employee access. IRS management agreed or partially agreed with seven of the eight recommendations and stated they either have or plan to implement corrective actions.



**TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION**

**U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024**

September 29, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements to the IRS’s Unauthorized Access
Program Could Further Protect Taxpayer Privacy
(Audit No.:2026300010)

This report presents the results of our review to assess the efficiency and effectiveness of the Internal Revenue Service’s unauthorized access program. This review is part of our Fiscal Year 2026 Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

Management’s complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Matthew A. Weir, Assistant Inspector General for Audit (Compliance and Enforcement Operations).

Table of Contents

Background	Page 1
-------------------------	--------

Results of Review	Page 3
--------------------------------	--------

<u>Additional Controls To Prevent and Detect Unauthorized Access Violations Need To Be Implemented</u>	Page 4
--	--------

<u>Recommendations 1 and 2:</u>	Page 6
---------------------------------------	--------

<u>Disciplinary Actions on Unauthorized Access Violations Need To Be Consistent and Emphasize Zero-Tolerance</u>	Page 6
--	--------

<u>Recommendation 3:</u>	Page 8
--------------------------------	--------

<u>Victim Notification Letters Were Not Always Provided to Impacted Taxpayers</u>	Page 9
---	--------

<u>Recommendations 4 and 5:</u>	Pages 10
---------------------------------------	----------

<u>Recommendation 6:</u>	Pages 11
--------------------------------	----------

<u>The IRS Has Not Established Executive Oversight of the Unauthorized Access Program</u>	Page 11
---	---------

<u>Recommendation 7:</u>	Page 12
--------------------------------	---------

<u>The IRS Should Improve the Performance Metrics for the Unauthorized Access Program</u>	Page 12
---	---------

<u>Recommendation 8:</u>	Page 12
--------------------------------	---------

Appendices

<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 13
--	---------

<u>Appendix II – Outcome Measures</u>	Page 14
---	---------

<u>Appendix III – Management’s Response to the Draft Report</u>	Page 15
---	---------

<u>Appendix IV – Glossary of Terms</u>	Page 20
--	---------

<u>Appendix V – Abbreviations</u>	Page 21
---	---------

Background

To perform their jobs, many Internal Revenue Service (IRS) employees need access to taxpayer account information. For example, an employee in the Taxpayer Services Division who answers taxpayer inquiries by phone or a revenue officer collecting on delinquent accounts needs access to taxpayer account information. IRS employees use the Integrated Data Retrieval System (IDRS) to access current information regarding taxpayer accounts.

For decades, stakeholders have been concerned about the problem of unauthorized employee access to taxpayer accounts. The Taxpayer Browsing Protection Act was signed into law on August 5, 1997, to address taxpayer information concerns. Specifically, the Taxpayer Browsing Protection Act made it unlawful for IRS employees to access or attempt to access taxpayer records unless there is a legitimate tax administration purpose. In May 2022, the Government Accountability Office issued a report determining that weaknesses in IRS data systems and processes persist that make taxpayer information vulnerable to both internal and external threats.¹

The willful, unauthorized access to taxpayer records can be punished criminally and civilly.² An unauthorized access conviction can result in fines up to \$1,000 and/or up to one year in prison, as well as termination of employment for federal employees. An unauthorized disclosure can result in fines up to \$5,000 and/or up to five years in prison as well as termination of employment for federal employees. The Taxpayer Browsing Protection Act also established the right of taxpayers to seek civil damages in a federal court. Even if the violation is not prosecuted by the Department of Justice, the employee is still subject to removal per IRS policy and under the Taxpayer Browsing Protection Act.

We have continued to report on weaknesses in IRS data systems that make the agency vulnerable to external and internal threats. For example, in 2025, we reported that the IRS's Cybersecurity program was considered not effective because three function areas were not at an acceptable maturity level.³ Vulnerabilities in the IRS's data systems have led to serious data breaches. For example, Charles Littlejohn, a contractor for the IRS, illegally obtained access to, and disclosed, tax returns and return information to media outlets. Littlejohn accessed more than 400,000 taxpayer accounts. Our Office of Investigations investigated this data breach and determined that Littlejohn was responsible. He was charged, pled guilty, and was sentenced to five years imprisonment.⁴

The unauthorized access, attempted access, or inspection of taxpayer records (UNAX) program was created to implement the requirements of the Taxpayer Browsing Protection Act.⁵ These requirements include educating IRS employees, systemically identifying potential violations, determining employee discipline when appropriate, and notifying victims. The mission of the

¹ Government Accountability Office, GAO-22-105872, *IRS Security of Taxpayer Information: Characteristics of Employee Unauthorized Access and Disclosure Cases*, p. 13 (May 2022).

² Internal Revenue Code Sections 7213, 7213A, and 7431.

³ TIGTA, Report No. 2025-200-037, *The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2025*, p. 4 (September 2025).

⁴ *United States v. Littlejohn*, 23-cr-0343 (D.D.C. 2023).

⁵ See Appendix IV for a glossary of terms.

UNAX program is to provide awareness to all IRS employees to ensure that they do not compromise public confidence by engaging in unauthorized access of taxpayer records.

Additionally, in the testimony leading up to the passage of the Taxpayer Browsing Protection Act, the Deputy Commissioner of the IRS pledged a zero-tolerance policy for substantiated UNAX violations.⁶ The IRS disciplinary guidelines also call for employee removal on substantiated UNAX cases without the taxpayer's knowledge or consent.

In June 2026, Senators introduced a bill to protect the privacy of American taxpayers' information. This bill, if passed, would establish new provisions increasing the criminal penalty for unauthorized disclosure of returns to a maximum fine of \$250,000 and up to seven years imprisonment. The bill would also establish a new felony offense for IRS contactors who willfully fail to enforce safeguards required under Internal Revenue Code (I.R.C.) Section (§) 6103 (e.g., the requirement to establish and maintain a permanent system of standardized records with respect to any request, the reason for such request, and the date of such request). The bill does not address unauthorized access without disclosure.

IRS offices responsible for administering UNAX

The IRS's Privacy Office (formerly known as the Privacy, Governmental Liaison and Disclosure program) has primary responsibility for establishing and administering UNAX policies. I.R.C. § 6103 provides protection for taxpayers' return information by limiting access to those who have a tax administration purpose. The Privacy Office administers service-wide policy, training, and communication for the UNAX program. Incident Management (IM) within the Privacy Office is responsible for sending notices to the victims of UNAX. Other areas of the IRS are involved in the UNAX process in addition to the Privacy Office, such as:

- Human Capital Office's (HCO) Employee Relations (ER) - advises IRS management about unauthorized access cases concerning IRS employees.
- Information Technology's, Cybersecurity - performs system tasks of detecting, reporting, and referring behavioral anomalies (e.g., questionable accesses, etc.) indicating potential UNAX violations to the Treasury Inspector General for Tax Administration (TIGTA) and IRS stakeholders.

IRS policy requires managers to take an active role in preventing willful and attempted unauthorized access and inspection of taxpayer information in both electronic and paper form. This includes overseeing employees' work and continually stressing the importance of protecting and securing taxpayer records.

Further, all IRS employees are responsible for protecting the confidentiality and privacy of taxpayer information. Employees are responsible for understanding what UNAX means and what the potential consequences are for willful UNAX violations. If they are uncertain whether access or inspection is appropriate, they should first consult a manager, TIGTA, or send questions to a designated UNAX organizational email address.

In addition, IRS policies provide that employees are only allowed to access tax return information when it is needed to carry out their assigned tax administration duties and there is

⁶ *IRS Mismanagement and Ideas for Improvement: Hearing Before the Subcomm. on Gov't Mgmt, Info., and Tech. of the H. Comm. on Gov't Reform and Oversight*, 105th Cong. 137 (1997) (statement of Michael P. Dolan, Deputy Commissioner, IRS).

no covered relationship.⁷ Employees have no legitimate tax-related reason to access any taxpayer account unless they receive the matter through official channels or in the normal course of performing their official job duties. Some examples include:

- Cases officially assigned by a manager for official IRS business purposes.
- Taxpayer walk-ins.
- Telephone calls from taxpayers.
- Official correspondence.
- Related case inquiries.

Results of Review

The inability to protect sensitive data may result in unauthorized access, disclosure, misuse, improper modification, or destruction of taxpayer information. This burdens affected taxpayers and violates their rights to confidentiality. Unauthorized access or disclosure can also erode public trust in the IRS, which may affect a taxpayer's decision to voluntarily comply with their tax obligations. We found the IRS's UNAX program is not adequately addressing the risk of unauthorized access to taxpayers' accounts. Specifically:

- Additional controls to prevent and detect unauthorized access violations need to be implemented.
- Disciplinary actions on UNAX violations need to be consistent and emphasize zero-tolerance.
- Victim notification letters were not always provided to impacted taxpayers.
- The IRS has not established executive oversight of the UNAX program.
- The IRS should improve the performance metrics for the UNAX program.

⁷ Covered relationships include spouse, ex-spouse, children, parents, grandparents, anyone living in household, close relatives, friends, neighbors, co-workers, supervisors, and other individuals an IRS employee may have a close personal or business relationship.

Figure 1 is an abbreviated summary of the key steps of the IRS UNAX program based on our conversations with staff from the Privacy Office and HCO-ER.

Figure 1: UNAX Program Process

Process	Responsible Entities/ Function(s)	Identified Risks
The detection process involves eight post access identification methods. Point of access controls include [REDACTED] and accounts blocked for taxpayers with respect to each IRS employee's covered relationships.	IRS Cybersecurity	Lack of Detection methods.
Suspected UNAX incidents are reported to TIGTA Office of Investigation (OI).	IRS Cybersecurity/ TIGTA OI, IRS Management	
TIGTA OI Investigates potential UNAX incidents and refers case to the Department of Justice or returns the matter to the IRS.	TIGTA OI	
TIGTA provides a Report of Investigation to the IRS-HCO.	TIGTA OI/HCO	
HCO prepares case file and completes a preliminary case analysis and sends it to Employee Relations (ER).	HCO-ER	
HCO-ER forwards the case file to IRS Management for determination of appropriate action.	HCO-ER/ Management	
IRS Management assisted by HCO determines appropriate discipline and sends request for action to IRS-HCO.	HCO-ER/ Management	Lack of appropriate discipline.
Proposed discipline letter is prepared and issued.	HCO-ER/IRS Management	
HCO discusses employee response along with Douglas Factors with deciding management official and prepares decision letter for issuance.	HCO-ER/IRS Management	Lack of appropriate discipline.
Management issues decision letter to the employee and initiates personnel action request.	HCO-ER/IRS Management	
ER notifies Privacy (Incident Management) of the completed investigation via email.	HCO-ER, Privacy	Lack of notification (or timely notification) to impacted taxpayers.
The Privacy Analyst prepares and sends the required victim notification letter to the impacted taxpayer whose records were accessed.	Privacy	Lack of notification to impacted taxpayers.

Source: Analysis of the IRS UNAX program.

Additional Controls To Prevent and Detect Unauthorized Access Violations Need To Be Implemented

The primary method to ensure that employee access to taxpayer information aligns with job duties is role-based access control, which restricts access to tax return information based on an employee's specific IRS function and business need. However, when authorized employees access IDRS there are no systemic controls to limit their access to only assigned taxpayers accounts. The lack of preventative control results in the risk of an IRS employee accessing an unauthorized tax account that may go undetected.

The IRS's Cybersecurity function employs various "use cases" designed to prevent employees from engaging in unauthorized browsing of taxpayer data, (e.g., review of a family member's tax information). When an employee attempts or accesses a family member's tax information (covered relationship), the Cybersecurity function is alerted and reports the suspected UNAX violation to our Office of Investigations. The IRS should study systemic improvements that will enable the IRS to expand preventative controls to reduce UNAX occurrences.

There are generally no additional access controls or detection methods to protect public officials or celebrities tax accounts

IRS does not have a mechanism to prevent or systemically detect browsing of celebrities. The IRS defines a celebrity as a person who is famous, widely known, or frequently in the media/of media interest, (e.g., music industry, sports, entertainment, etc.). The IRS does not maintain a comprehensive list to help prevent unauthorized access of public officials or celebrities. After the *Littlejohn* case, Cybersecurity management implemented controls that provide post access alerts, (i.e., after access notifications regarding [REDACTED] accessed). Thus, the technology is available for the IRS to consider adding a similar post access control to the tax information of celebrities.

Suspicious accesses using command code NAMES are not being prevented or detected

We found that the use of certain IDRS command codes circumvents the ability of the Cybersecurity function to detect some unauthorized uses. IDRS user profiles are created based on the command codes that are available to the IDRS unit. The unit profile contains all the command codes that users in that unit are authorized to have. The employee profile only contains a subset of command codes that are in the unit's profile.

With very few exceptions, IDRS queries use command codes that require knowledge and input of the Taxpayer Identification Number (TIN) (e.g., Employer Identification Number or Social Security Number). However, there are some command codes that use the first ten characters of the taxpayer's last name to retrieve the taxpayer's TIN. The IDRS command codes used for these queries include the NAMEB and NAMEI command codes (hereafter referred to as NAMES).⁸ The employee may use a taxpayer's name and address, if known, to identify the taxpayer's TIN.

Further, the use of the command code NAMES bypasses the current IRS monitoring methods used for identifying UNAX accesses. As a result, the use of NAMES can obtain taxpayer information such as a TIN and address as the initial step to committing potential fraud or identity theft. This could be done without any IRS detection under existing controls.

We reviewed the IDRS audit logs that included almost 6 million IDRS searches using the NAMES command code from Calendar Years 2022 through 2025 (as of November 2025). Using a limited number of high-profile taxpayer names of United States government officials, business leaders and entertainers, we identified 86 suspicious accesses by IRS employees (e.g., Contact Service Representatives and Tax Examining Technicians).

The 86 suspicious accesses involved 30 different taxpayer accounts belonging to high-profile taxpayers. An example of a suspicious access would be a Customer Service Representative searching for a prominent business leader using the NAMES command code. Taxpayers of this nature do not typically engage with the IRS without formal documentation or an open case file that would include their respective TIN. These suspicious accesses were not identified by the IRS and therefore not referred to our Office of Investigations for investigation. Privacy Office officials could not provide a business purpose as to why the 52 employees accessed the tax accounts of government officials, business leaders, and entertainers. We have referred the 86 suspicious

⁸ IDRS command codes NAMES, NAMEE, NAMEI, and NAMEB were developed to allow users to do research on the IDRS for entity data. Entity data consists of the portion of the Master File record which identifies the taxpayer, including the taxpayer's name, address and Social Security Number or Employer Identification Number.

accesses to our Office of Investigations for further action.

We determined that there are no systemic preventative or monitoring controls for the use of the NAMES command codes. In addition, the NAMES command codes are not classified as sensitive. Sensitive command codes allow employees to perform IDRS actions that warrant increased management oversight. For example, specific sensitive command codes can be used to adjust account balances, change the status of a tax module, or affect the tax liability. Not only do these changes alter the tax account, but they may also be used for fraudulent activity. Since command code NAMES performs research, it does not meet the criteria to be considered a sensitive command code. However, permitting IRS employees to use the NAMES command codes without preventative or monitoring controls may allow employees to gain unauthorized access to taxpayer data. Thus, the IRS should develop and implement controls to mitigate this risk. Potential controls to be considered would be reducing the number of employees with NAMES command code access and establishing preventative role-based access controls aligned with job duties.

Overall, the IRS lacks preventative controls to stop unauthorized access and has not effectively identified suspicious unauthorized accesses post access. Existing preventative controls are primarily limited to accounts of family or close relations. Finally, the IRS does not have a mechanism to prevent or systemically detect browsing of celebrities or public officials.

The Chief Privacy Officer should:

Recommendation 1: Study systemic improvements that will enable the IRS to implement preventative controls to prevent UNAX occurrences.

Management's Response: IRS management agreed with this recommendation. The Privacy Office will study and document findings for systemic enhancements to strengthen preventative controls that reduce the risk of UNAX violations.

Recommendation 2: Develop and implement controls such as reducing the number of employees with NAMES command code access and post access monitoring that identifies suspicious NAMES command code accesses.

Management's Response: IRS management agreed with this recommendation. The Privacy Office will develop and document requirements to strengthen governance over NAMES command code access and post access monitoring. Upon finalization of the requirements, Privacy will share with the appropriate stakeholders, as needed, for review and decision on implementation of necessary system changes, access restrictions, and monitoring capabilities.

Disciplinary Actions on Unauthorized Access Violations Need To Be Consistent and Emphasize Zero-Tolerance

We reviewed the Automated Labor and Employee Relations Tracking System data for Fiscal Years (FY) 2023 through 2025 and identified 53 cases in which an employee accessed a

taxpayer's account without their knowledge or consent.⁹ For 31 (58 percent) of the 53 cases, the employee was terminated. However, in the remaining 22 (42 percent) cases, the employee was not terminated. For 13 of these 22 cases, the deciding official cited length of service and first-time offense as the reason not to terminate the employee. However, all 22 of these employees received some form of discipline, ranging from suspensions to reprimands. Some examples of the UNAX violations include:

[REDACTED]

As shown in Figure 2, the IRS Manager's Guide to Penalty Determinations (Penalty Guide) provides for an employee's removal if an unauthorized access of tax return or tax information was committed without the taxpayer's knowledge and consent. By not removing these 22 employees, the IRS may not be following a zero-tolerance standard and may not be reinforcing the importance of avoiding UNAX violations. Furthermore, by retaining these 22 employees, the IRS is taking unnecessary risks for additional UNAX violations by either a repeat offender or by an employee who perceives the lack of punishment as a low barrier to committing UNAX's.

Figure 2: IRS Manager's Guide to Penalty Determinations (Excerpt)

Nature of Offense	First Offense	Key Penalty Factors
Unauthorized access of tax return or tax information without the taxpayer's knowledge and consent. The employee breached the taxpayer's rights, the UNAX policy, and the intent of the Taxpayer Browsing Protection Act.	Removal	Accesses were outside official channels and tasks performed were not otherwise within the employee's official duties. Examples of types of accesses may include: • Employees accessed an account out of curiosity. • Employees sought to locate spouse or ex-spouse, family members or close friends.

Source: IRS Manager's Guide to Penalty Determinations.

We discussed our concern about whether the IRS is achieving a zero-tolerance policy with HCO management officials. They stated that the IRS is following a zero-tolerance standard by referring all UNAX cases for investigation. The IRS discipline process involves the application of the Douglas Factors, (*i.e.*, case law factors used to weigh the appropriateness of punishment for misconduct).¹⁰

By applying the Douglas Factors, employees may receive lesser punishment than removal. Examples of these factors include the seriousness of the offense and whether it was intentional. The three examples we provided above were serious and intentional, and we would expect that

⁹ The IRS uses the Automated Labor and Employee Relations Tracking System for tracking labor and employee relations case data.

¹⁰ *Douglas v. Veterans Administration*, 5 M.S.P.R. 280 (1981).

a zero-tolerance policy would have resulted in the removal of those employees. Also, proper application of the Douglas Factors requires consistency of the penalty with those imposed upon other employees for the same or similar offenses. When we highlighted that the Penalty Guide only reflects removal as an option for the first UNAX offense, HCO officials stated that adherence to this document is not a requirement and only serves as a guide.

HCO officials also stated that they have experienced reversals of UNAX-related removal decisions by the Merit Systems Protection Board (MSPB).¹¹ When asked for evidence of prior MSPB UNAX reversal decisions, the IRS only provided one case from 2002. The facts in this case were that management made numerous procedural errors in its consideration of the case.¹² We found other cases that showed that MSPB sustained IRS UNAX removal decisions, even in instances of a first offense where employees have otherwise been performing satisfactorily.¹³

IRS Counsel stressed that the correct application of the Douglas Factors means that management cannot have a predetermined outcome of removal of the employee before the application of the factors. IRS Counsel also noted that the IRS management must consider mitigating factors and aggravating circumstances as required by the law. In addition, HCO officials agreed that consistency in the application of the Douglas Factors is imperative and that the most important factor to consider is the first one (*i.e.*, the nature and seriousness of the offense). Consideration of this factor recognizes that removal may be the correct remedy given the seriousness of the misconduct, even on the first offense.

The public relies on the ethics and integrity of IRS employees to ensure that their tax information is protected from an unauthorized access and/or disclosure. Further, the IRS has determined that UNAX violations are a serious threat to the integrity of tax administration. The employees who do not uphold these standards when performing their duties should face serious discipline including removal when appropriate. Discipline consistent with the IRS Penalty Guide will ensure that taxpayers can trust that the information provided to the IRS will be protected and only used for legitimate tax administration purposes. On July 2, 2026, a new rule was proposed jointly by the Office of Personnel Management and the MSPB to no longer apply the Douglas Factors to improve accountability of employees for poor performance and misconduct.¹⁴

Recommendation 3: The IRS HCO, Director, Human Resources Operations and Shared Services should clarify guidance on the application of the Douglas Factors emphasizing that managers afford the proper weight in intentional UNAX cases to the nature and seriousness of the offense in cases of serious misconduct.

Management's Response: IRS management agreed with this recommendation. The HCO will clarify guidance on determining the appropriate discipline in cases of serious misconduct, including intentional UNAX cases.

¹¹ Employees who receive a proposal to remove can bring their case before the MSPB.

¹² *Brown v. Dept. of Treasury*, 91 MSPR 60 (February 15, 2002). The MSPB found that management treated years of lengthy service as an aggravating factor rather than a mitigating factor and failed to consider a lesser penalty.

¹³ While there are numerous such decisions where the MSPB sustains the decision to remove IRS employees in UNAX cases, some of the MSPB decisions reviewed include: *Pope v. Dept. Treasury*, No. DA-0752-06-0663-1-1 (December 22, 2006); *Reese v. Dept. of Treasury*, No. DA-0752-12-0479-1-1 (September 25, 2012); *Romona v. Dept. of Treasury*, No. PH-0752-22-0177-1-1 (June 30, 2022).

¹⁴ *Promoting Employee Accountability*, 91 Fed. Reg. 40444 (proposed July 2, 2026) p. 1.

Victim Notification Letters Were Not Always Provided to Impacted Taxpayers

The I.R.C. requires the IRS to notify taxpayers whose personal information was intentionally accessed or disclosed without authorization as soon as practicable after an employee is criminally charged or if discipline is proposed.¹⁵ Without the I.R.C. § 7431(e) notifications, many taxpayers whose data has been improperly browsed or disclosed might never otherwise learn of it. When taxpayers are notified, they can take steps to protect themselves from potential financial harm (*e.g.*, credit monitoring against potential identify theft). From FYs 2023 through 2025, the IRS closed 122 UNAX cases.

We reviewed these cases to determine if the impacted taxpayers were notified of the IRS employees' unauthorized access to their tax information. We found that the IRS properly notified 64 taxpayers in 39 (32 percent) of 122 cases. However, in the remaining 83 cases (68 percent), the IRS did not notify a total of 276 taxpayers. Specifically, the IRS:

- Failed to notify 175 taxpayers of unauthorized access to their tax records due to an employee not following procedures in 42 out of 83 cases. This occurred because HCO-ER failed to send the TIGTA Report of Investigation, proposal, and decision letters to the Privacy Office-IM or confirm receipt, as outlined in their procedures.¹⁶ As a result, these 175 victims did not have an opportunity to take precautions to protect themselves from potential financial harm. The IRS agreed that the 175 taxpayers should have been notified.
- Failed to notify 101 taxpayers of unauthorized access to their tax records due to IRS policy in 41 out of 83 cases. This occurred because the IRS only requires taxpayer notification when employee discipline is proposed.¹⁷ The IRS employees responsible for these 41 cases either resigned or retired before disciplinary action was proposed. As a result, these 101 victims did not have an opportunity to take precautions to protect themselves from potential financial harm.

The IRS did not always timely notify taxpayers when their tax records were accessed by an unauthorized employee

We reviewed the 39 UNAX cases in which the IRS notified the 64 taxpayers of unauthorized access to determine the timeliness of the victim notices sent. I.R.C. § 7431(e) requires notification of impacted taxpayers as soon as practicable after an employee is disciplined or criminally charged. However, the IRS has not defined or established a time frame to comply with the I.R.C. § 7431(e) requirement. Accordingly, we applied a standard for notification within 30 days after proposed disciplinary action for the employee.¹⁸ We determined that the IRS victim notification process does not always timely notify impacted taxpayers. We found that in 26 (67 percent) of the 39 cases, 40 taxpayers received their notification more than 30 days after the proposed disciplinary action for the employee. For the remaining 13 (33 percent) of the

¹⁵ I.R.C. § 7431(e).

¹⁶ A TIGTA Report of Investigation is a document summarizing the results of the UNAX investigation. The proposal letter is sent to the employee explaining the proposed discipline. The decision letter contains the final disciplinary action.

¹⁷ I.R.C. § 7431 requires taxpayer notification when employee discipline is proposed.

¹⁸ We used 30 days because it is a common standard applied by the IRS.

39 cases, the IRS timely provided notification to the 24 impacted taxpayers. Figure 3 shows the time frames it took the IRS to notify the 64 impacted taxpayers.

Figure 3: Timeliness of Notices

UNAX Cases	Taxpayers Impacted	Time Range
13	24	0 – 30 days
18	24	31 – 365 days
■	■	366 – 1,000 days
■	11	1,001 and 1,423 days

Source: Analysis of IRS data on the timing of sending notices to impacted taxpayers.

Timely notification of taxpayers is critical to minimize the adverse impact the unauthorized access may have on the taxpayer. Given the potential risk that the taxpayer's data may be used to commit a crime or fraud, impacted taxpayers need to be notified timely so they can minimize this impact (e.g., obtain identity protection and identity monitoring services). No notice or untimely notice prevents these taxpayers from taking protective steps in response to an unlawful IRS employee action(s).

For instance, in the previously discussed *Littlejohn* case, criminal charges were brought by the Department of Justice in September 2023. However, the required victim notifications for some of the victims were not sent until December 2024. In some cases, untimely victim notification can result in victims not receiving notification at all. Our Office of Inspection and Evaluations report identified 12,200 undelivered victim notices related to the data breach in the *Littlejohn* case, which were returned to the IRS from the U.S. Postal Service as undeliverable.¹⁹

The Chief Privacy Officer official should:

Recommendation 4: Immediately notify the 276 impacted taxpayers identified during this audit of unauthorized access to their tax information.

Management's Response: The IRS partially agreed with this recommendation. IRS management stated that the Privacy Office reviewed 54 Reports of Investigation, and as a result, 182 taxpayers were notified.

Office of Audit Comment: The IRS's response substantially complies with our recommendation. Notification of the remaining taxpayers is dependent on the outcome of the IRS's review of its legal authorities as discussed in Recommendation 6.

Recommendation 5: Establish overall timeliness standards regarding victim notifications to impacted taxpayers per I.R.C. § 7431(e)(3).

Management's Response: IRS management disagreed with this recommendation and stated that they have timeliness standards from the time Reports of Investigations are received to the time the impacted taxpayers are notified.

¹⁹ TIGTA, Report No. 2025-IE-R019 *Thousands of Notifications to Taxpayers Affected by the Large-Scale Data Breach Were Returned Undeliverable*, p. 2 (May 2025). The U.S. Postal Service may include an explanation as to why mail is being returned as undeliverable, such as forwarding order expired or undeliverable as addressed.

Office of Audit Comment: During this review, the IRS agreed to our recommendation that a timeliness standard was needed. However, at the close of our review, the IRS provided internal procedures that included a 30-day taxpayer notification standard which broadly applies to data breaches involving personally identifiable information, *e.g.*, when the IRS loses or misplaces taxpayer information. While the data breach notification standards cover some UNAX cases, they specifically do not cover all I.R.C. § 7431(e) notifications, *i.e.*, where there has been a criminal indictment. Therefore, we continue to believe a specific timeliness standard for all UNAX cases is still needed. As previously noted, our review found a 67 percent failure rate to notify victims within 30 days, showing that the IRS is not following its current standard.

Recommendation 6: Work with the Office of Chief Counsel on determining whether existing law would allow a new process to be developed that ensures all taxpayers are notified of willful unauthorized access to their records when a violation has been confirmed regardless of employee discipline status, (*i.e.*, even if the employee has resigned or retired). If a change in the law is not required, the IRS should develop a new process. If the Office of Chief Counsel determines a change in I.R.C. § 7431(e)(3) is required, work with the Treasury Office of Tax Policy to request an appropriate legislative change.

Management's Response: IRS management partially agreed with this recommendation and stated that they consistently notify taxpayers in accordance with regulations of UNAX. However, the Privacy Office agreed to request a legal opinion from the Office of Chief Counsel to determine whether existing law permits the development of a new process to notify all taxpayers of confirmed willful UNAX regardless of the employee's discipline or employment status. Lastly, IRS management stated that, based on Chief Counsel's determination, they will develop an appropriate notification process.

Office of Audit Comment: The IRS's response substantially complies with the recommendation.

The IRS Has Not Established Executive Oversight of the Unauthorized Access Program

The UNAX program involves multiple areas of the IRS with no executive with overall authority and responsibility to ensure that the UNAX program is working to protect taxpayers' personal information. As previously stated, the Privacy Office has responsibility for UNAX policies and has specific roles in the process. However, the Privacy Office lacks the authority to define the roles and responsibilities of the other IRS functions that participate in the UNAX program.

The Office of Management and Budget's (OMB) guidance on management's responsibility for internal controls establishes requirements for assessing, reporting, and maintaining effective internal controls.²⁰ OMB guidance requires agency executives to have overall responsibility for establishing the organization's system of internal control, including: (1) ensuring an efficient and effective system of internal control; (2) establishing a system of internal control review; (3) documenting the system of internal control and making policies and guidelines available to

²⁰ OMB Circular No. A-123.

all employees; and (4) implementing education and training about the system of internal controls, related to topics including risk, internal control, and internal control evaluations.

The IRS has not established or designated an executive to have UNAX oversight responsibilities consistent with the OMB guidance. Without establishing executive oversight of the UNAX program and its activities, the IRS is limited in its ability to make risk decisions across the agency regarding how to most effectively ensure that the UNAX program is protecting taxpayer information. In addition, the IRS lacks the ability to reduce the likelihood that adverse events will occur such as the deficiencies we identified during our audit previously discussed.

Recommendation 7: The Chief Executive Officer should designate a senior official with full oversight responsibility over the UNAX program.

Management's Response: IRS management agreed with this recommendation and stated that the IRS Chief Executive Officer designated the Chief Privacy Officer as the senior official with full oversight responsibility over the UNAX program.

The IRS Should Improve the Performance Metrics for the Unauthorized Access Program

The IRS currently has metrics for employee UNAX cases closed, average days to close a UNAX investigation, and contractor UNAX cases closed. However, we determined that the IRS has not established or defined performance metrics to ensure that:

- The victims of unauthorized UNAX violations are timely notified.
- Disciplinary actions for unauthorized UNAX violations are consistent after proper application of the Douglas Factors.

OMB provides that agencies should establish a clear and transparent reporting system to communicate the results of internal control activities to senior leadership and relevant oversight bodies, such as the agency Inspector General. In addition, the reporting system should ensure that information is presented in a timely manner and consistent and understandable format. Further, the reporting system should highlight key internal control findings, performance metrics, and risk areas requiring attention or improvement.

Establishing performance metrics for the UNAX program would assist the IRS in achieving its goal of protecting taxpayer information and to effectively mitigate potential risks to unauthorized accesses. Privacy Office leadership agreed that performance metrics should be enhanced and will be coordinated with HCO and Information Technology to improve the performance metrics for the UNAX program.

Recommendation 8: The Chief Privacy Officer should enhance business performance metrics for the UNAX program.

Management's Response: IRS management agreed with this recommendation. The Privacy Office will assess the current UNAX performance measurement framework and enhance business performance metrics, as appropriate, to strengthen program oversight, improve accountability, and support continuous program improvement.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the efficiency and effectiveness of the IRS's unauthorized access program. To accomplish our objective, we:

- Reviewed the IRS process for identifying UNAX violations including the detection of celebrities and government officials.
- Reviewed IRS audit logs for suspicious access using the NAMEI command codes.
- Determined whether the final discipline of employees who browse taxpayer information without authorization was in accordance with a zero-tolerance policy.
- Determined if taxpayers were sent required notices when an IRS employee accessed their tax accounts without authorization.
- Reviewed the IRS UNAX flowchart to determine how potential UNAX violations flow from identification to disposition of the case.

Performance of This Review

This review was performed with information obtained from the Privacy Office located at IRS National Headquarters in Washington, D.C., during the period July 2025 through June 2026. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Data Validation Methodology

We performed tests to assess the reliability of data from the IRS Automated Labor and Employee Relations Tracking System database and TIGTA's Data Center Warehouse. We evaluated the data by (1) performing electronic testing of required data elements and (2) reviewing existing information about the data and the system that produced them. We determined that the data was sufficiently reliable.

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 objective: IRS policies, procedures and practices for preventing, detecting, disciplining employees and notifying victims of IRS employee browsing.

Appendix II

Outcome Measures

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:

- Taxpayers Impacted - Potential; 175 taxpayers who the IRS failed to notify of IRS employees' unauthorized access to their tax records due to employees not following procedures. (see Recommendations 4 and 6).

Methodology Used to Measure the Reported Benefit:

We reviewed 122 UNAX cases for review that were closed from FY 2023 through FY 2025 to determine if the impacted taxpayers were notified of an IRS employees' unauthorized access to their tax records. We determined the IRS failed to notify 175 taxpayers of unauthorized access to their tax records due to employees not following procedures in 42 out of 122 cases.

Type and Value of Outcome Measure:

- Taxpayers Impacted - Potential; 101 taxpayers who the IRS failed to notify of IRS employees' unauthorized access to their tax records due to a breakdown of current policy. (see Recommendations 4 and 6).

Methodology Used to Measure the Reported Benefit:

We reviewed 122 UNAX cases for review that were closed from FY 2023 through FY 2025 to determine if the impacted taxpayers were notified of an IRS employees' unauthorized access to their tax records. We determined that the IRS failed did not notify 101 taxpayers of unauthorized access to their tax records due to current policy in 41 out of 122 cases.

Appendix III

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 16, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: John J. Walker
Acting Chief Privacy Officer John J. Walker

SUBJECT: Draft Audit Report – Audit No. 2026300010, Improvements to the IRS's Unauthorized Access Program Could Further Protect Taxpayer Privacy.

Digitally signed by John J.
Walker
Date: 2026.09.16 14:17:21
-04'00'

Thank you for the opportunity to respond to the draft report, *Improvements to the IRS's Unauthorized Access Program Could Further Protect Taxpayer Privacy*, Audit No. 2026300010.

The Internal Revenue Service (IRS) remains firmly committed to safeguarding taxpayer information and continuously strengthening the Unauthorized Access of Taxpayer Accounts (UNAX) program through effective oversight, risk management, and process improvements designed to protect taxpayer privacy and maintain public trust.

We appreciate the Treasury Inspector General for Tax Administration's review and the opportunities to further enhance the program. The IRS has carefully evaluated each recommendation and will implement appropriate corrective actions while continuing to administer the UNAX program in accordance with Internal Revenue Code section 7431 and other applicable laws to protect taxpayer information.

Our detailed response to each recommendation, including the corrective action plan and implementation date, is attached.

If you have any questions, please contact me at (267) 466-2416, or a member of your staff may contact Stephen Brooks, Acting Director, Data Oversight & Records, at (240) 613-3210.

Attachment

Attachment

**Improvements to the IRS's Unauthorized Access Program Could Further Protect
Taxpayer Privacy
Audit No. 2026300010**

RECOMMENDATION 1:

The Chief Privacy Officer should study systemic improvements that will enable the IRS to implement preventative controls to prevent UNAX occurrences.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Privacy Office will study and document findings for systemic enhancements to strengthen preventive controls that reduce the risk of Unauthorized Access (UNAX) violations.

IMPLEMENTATION DATE:

April 5, 2027

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer

RECOMMENDATION 2:

The Chief Privacy Officer should Develop and implement controls such as reducing the number of employees with NAMES command code access and post access monitoring that identifies suspicious NAMES command code accesses.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Privacy Office will develop and document requirements to strengthen governance over NAMES command code access and post access monitoring. Upon finalization of the requirements, Privacy will share with the appropriate stakeholders, as needed for review and decision on implementation of necessary system changes, access restrictions, and monitoring capabilities.

IMPLEMENTATION DATE:

May 29, 2027

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer and Chief Information Officer

RECOMMENDATION 3:

The IRS HCO, Director, Human Resources Operations and Shared Services should clarify guidance on the application of the Douglas Factors emphasizing that managers afford the proper weight in intentional UNAX cases to the nature and seriousness of the offense in cases of serious misconduct.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Human Capital Office (HCO) will clarify guidance on determining the appropriate discipline in cases of serious misconduct, including intentional UNAX cases.

IMPLEMENTATION DATE:

December 7, 2026

RESPONSIBLE OFFICIAL(S):

HCO, Director, Human Resources Operations and Shared Services

RECOMMENDATION 4:

The Chief Privacy Officer should immediately notify the 276 impacted taxpayers identified during this audit of unauthorized access to their tax information.

CORRECTIVE ACTION:

The IRS partially agrees with this recommendation. The Privacy Office reviewed 54 Reports of Investigation (ROIs), as a result of the review, 182 taxpayers were notified.

IMPLEMENTATION DATE:

Implemented

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer

RECOMMENDATION 5:

The Chief Privacy Officer should establish overall timeliness standards regarding victim notifications to impacted taxpayers per I.R.C. § 7431(e)(3).

CORRECTIVE ACTION:

The IRS disagrees with this recommendation. The IRS has timeliness standards from the time the Reports of Investigations is received to the time the impacted taxpayers are notified.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer (Privacy)

RECOMMENDATION 6:

The Chief Privacy Officer should work with the Office of Chief Counsel on determining whether existing law would allow a new process to be developed that ensures all taxpayers are notified of willful unauthorized access to their records when a violation has been confirmed regardless of employee discipline status, (i.e., even if the employee has resigned or retired). If a change in the law is not required, the IRS should develop a new process. If the Office of Chief Counsel determines a change in I.R.C. § 7431(e)(3) is required, work with the Treasury Office of Tax Policy to request an appropriate legislative change.

CORRECTIVE ACTION:

The IRS partially agrees with this recommendation. The IRS consistently notifies tax payers in accordance with regulations of unauthorized access. However, the Privacy Office agrees to request a legal opinion from the Office of Chief Counsel to determine whether existing law permits the development of a new process to notify all taxpayers of confirmed willful unauthorized access regardless of the employee's discipline or employment status. Based on Chief Counsel's determination, the IRS will develop an appropriate notification process.

IMPLEMENTATION DATE:

December 1, 2026

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer (Privacy)

RECOMMENDATION 7:

The Chief Executive Officer should designate a senior official with full oversight responsibility over the UNAX program.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The IRS Chief Executive Officer (CEO) designated the Chief Privacy Officer as the senior official with full oversight responsibility over the UNAX program.

IMPLEMENTATION DATE:

Implemented

RESPONSIBLE OFFICIAL(S):

Chief Executive Officer

RECOMMENDATION 8:

The Chief Privacy Officer should enhance business performance metrics for the UNAX program.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Privacy office will assess the current UNAX performance measurement framework and enhance business performance metrics, as appropriate, to strengthen program oversight, improve accountability, and support continuous program improvement.

IMPLEMENTATION DATE:

December 1, 2026

RESPONSIBLE OFFICIAL(S):

Chief Privacy Officer (Privacy)

Appendix IV

Glossary of Terms

Term	Definition
Automated Labor and Employee Relations Tracking System	An application used to track labor/employee relations case data. It was developed to ensure consistency in tracking labor and employee relations disciplinary actions.
Covered Relationships	Personal or outside business relationships that can raise questions about the employee's impartiality in the handling of a tax matter.
Employee	Includes all IRS personnel. Also includes all contractors who have staff-like access.
Employer Identification Number	A unique, nine-digit number used to identify a taxpayer's business account.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The federal government's fiscal year begins on October 1 and ends on September 30.
Inspection	The terms "inspected" and "inspection" mean any observation, review, or examination of a return or return information (paper or electronic).
Staff-Like Access	This is when a contracted individual is granted access to IRS facilities or IRS systems or has opportunity to be exposed to IRS information.
Taxpayer Identification Number	A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, it can be an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.
UNAX	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.
Zero-Tolerance	Substantiated unauthorized access, absent mitigating circumstances, will result in their removal from the IRS.

Appendix V

Abbreviations

ER	Employee Relations
FY	Fiscal Year
GAO	Government Accountability Office
HCO	Human Capital Office
IDRS	Integrated Data Retrieval System
IM	Incident Management
I.R.C.	Internal Revenue Code
IRS	Internal Revenue Service
MSPB	Merit Systems Protection Board
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
UNAX	Unauthorized Access (Browsing)



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

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

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