TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information

February 6, 2024

Report Number: 2024-IE-R008

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

HIGHLIGHTS: Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information

Final Evaluation Report issued on February 6, 2024 **Report Number 2024-IE-R008**

Why TIGTA Did This Evaluation

In February 2023, the Chairman of the U.S. House Ways and Means Committee sent a letter to TIGTA that referenced a news media outlet that, in June 2021, revealed a "massive leak of confidential tax information that the IRS is charged with keeping secure". At the time, the news media outlet stated that it had "obtained a vast trove of Internal Revenue Service data on the tax returns of thousands of the nation's wealthiest people, covering more than 15 years."

Subsequent to receipt of the Chairman's letter, TIGTA agreed to conduct an evaluation addressing how the IRS grants access to and safeguards Federal Tax Information maintained on its various information technology systems (*i.e.*, sensitive systems).

Impact on Tax Administration

Unauthorized access and disclosure of taxpayer information could undermine the taxpaying public's trust in the Federal tax system to safeguard confidential tax information.

What TIGTA Found

TIGTA identified that users are granted access to sensitive systems via the Business Entitlement Access Request System (BEARS) application and that the process is the same for employees and contractors. As of July 13, 2023, our evaluation identified a total of 91,661 users, of which 5,068 were contractors, who were authorized to access one or more of the 276 sensitive systems specific to our evaluation. Procedures to systemically remove users who no longer require access to sensitive systems were not always working as intended. For example, TIGTA identified 279 users who were listed in BEARS as separated who, as of July 13, 2023, continued to have access to at least one IRS sensitive system. However, for each of these individuals IRS network access was removed, which according to the IRS, reduces, but does not eliminate, the risk that a user can access a sensitive system.

The IRS did not always remove contractor access to sensitive systems when background investigations were not favorable. Specifically, 19 contractors' most recent background investigations were not favorable as of July 13, 2023. However, these contractors still retained their access to one or more sensitive systems because the IRS did not take action to suspend or disable the contractors from the IRS's systems, as required.

Finally, the IRS is evaluating steps to improve its ability to safeguard data housed on its sensitive systems. These steps include identifying and recording user actions when accessing sensitive data and tracking authorized and unauthorized attempts of removal of sensitive data from its systems. A key initiative is the IRS's Compliance Data Warehouse enhanced data security project that will enhance security controls for user access and data exporting of Federal Tax Information from certain IRS systems.

However, for some sensitive systems, the IRS does not have adequate controls to detect or prevent the unauthorized removal of data by users. TIGTA has reported that a key deficiency in the IRS's detection and deterrence processes did not ensure that all sensitive systems provide complete, accurate, and usable audit trail logs for monitoring and identifying unauthorized access and for other investigative purposes.

What TIGTA Recommended

TIGTA made three recommendations that included ensuring that access to sensitive systems is immediately suspended when a contractor is identified as not having a favorable background investigation determination and ensuring that user network and sensitive system access are timely removed for users who separate from the IRS. The IRS agreed with all three recommendations.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: February 6, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Russell P. Martin
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Report – Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information (Evaluation # IE-23-026)

This report presents the results of our review to assess user access to taxpayer information maintained by the Internal Revenue Service (IRS) and identify the number of IRS systems that contain taxpayer information. In February 2023, the Chairman sent a letter to the Treasury Inspector General for Tax Administration (TIGTA) that referenced a news media outlet that, in June 2021, revealed a "massive leak of confidential tax information that the IRS is charged with keeping secure". Subsequent to our receipt of the Chairman's letter, TIGTA agreed to conduct an evaluation addressing how the IRS grants access to and safeguards Federal Tax Information maintained on its various information technology systems. This review was not included in our Fiscal Year 2023 Program Plan. This evaluation addresses the issue of access to taxpayer information maintained by the IRS and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources*.

Management's complete response to the draft report is included as Appendix III. In their response, management concurred with all three recommendations and identified their corrective actions; however, management also summarized their concerns with TIGTA's characterization of the IRS's current security posture. Our response to management's concerns is provided in Appendix IV.

Table of Contents

Background

In February 2023, the Chairman sent a letter to the Inspector General for the Treasury Inspector General for Tax Administration (TIGTA), that referenced a news media outlet that, in June 2021, revealed a "massive leak of confidential tax information that the IRS is charged with keeping secure". At the time, the news media outlet stated that it had "obtained a vast trove of Internal Revenue Service data on the tax returns of thousands of the nation's wealthiest people, covering more than 15 years," and subsequently published a series of articles focusing on numerous American taxpayers.

Following our receipt of the Chairman's letter, TIGTA agreed to conduct an evaluation addressing how the IRS grants access to and safeguards Federal Tax Information (FTI) maintained on its various information technology systems (hereafter referred to as "sensitive systems").[1] FTI refers to a returns and return information protected from unauthorized disclosure under Internal Revenue Code § 6103.[2] According to the Internal Revenue Code § 6103, return information includes, among other things, a taxpayer's identity, the nature or amount of their income, deductions, exemptions, assets, liabilities, net worth, tax withheld, or tax payments under Title 26.

Unauthorized access and disclosure of taxpayer information could undermine the taxpaying public's trust in the Federal tax system to safeguard confidential tax information.

The IRS takes actions to strengthen processes and procedures for the safeguarding of FTI

In February 2021, the IRS began the process of converting the Online 5081 system it used to grant users access to its information technology systems to its new Business Entitlements Access Request System (BEARS).[3] IRS management notes that one key benefit of its new user access system is that BEARS includes the capability to systemically integrate with IRS data in the U.S. Department of the Treasury's personnel system (HRConnect). The IRS completed its migration to BEARS in August 2022.[4] BEARS is now the sole system the IRS uses to request, modify, and remove access to IRS information technology systems. BEARS is also used to recertify and validate user access as well as remove access for separated, furloughed, and inactive users from the system.

In addition, in response to the previously mentioned June 2021 news media outlet's reporting, the IRS initiated a review of its safeguarding of FTI and/or Personally Identifiable Information (PII) (hereafter referred to as "sensitive data") maintained on its numerous information technology systems. The IRS reported that its actions included:

[1] For the purposes of this review, sensitive systems include those systems that process Personally Identifiable Information, which includes FTI.

[2] 26 U.S.C. § 6103.

[3] See Appendix V for a glossary of terms.

[4] TIGTA, Report No. 2023-20-013, *The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed* (Mar. 2023).

- Reducing the number of users with access to its Compliance Data Warehouse (CDW) by about 25 percent. Specifically, the IRS removed nearly all users' access to this system. Users were then required to provide a documented business justification to show a continued need to access the CDW. In addition to documenting a business justification for continued need to access the CDW, executive-level approval was also required, with re-approval required on a recurring basis.
- Limiting access to information in the CDW. Specifically, data in the CDW are separated by domain (Individual, Business, *etc.*) and sensitivity level (PII/FTI, non-PII, *etc.*), and more specific permissions were implemented for each level of access.
- Improving the masking of sensitive data in the CDW. Masking involves removing or replacing aspects of sensitive data that one might trace back to specific taxpayers (*e.g.*, masking of Taxpayer Identification Numbers).
- Deactivating user access to specific systems after a specified period of inactivity.
- Improving the monitoring and event logging of user access to sensitive systems including creating and maintaining evidentiary copies of database queries and data outputs.
- Revising removable media storage device (*e.g.*, external hard drives, USB drives) policies to prohibit a user's ability to download data from an IRS information technology system onto an external storage device. Employees who need to download data to an external storage device must now seek executive-level approval.
- Standing up a new steering committee process for enhancing data security. The goal of the committee is to enhance security and monitoring controls for user access and data when exporting FTI from Research, Applied Analytics, and Statistics (RAAS) systems.

Incomplete list of sensitive systems limited our assessment

The focus of this evaluation includes assessing the IRS's processes and procedures to permit employee and contractor access to sensitive systems and once permitted access, how well the IRS safeguards information on these sensitive systems. To perform this evaluation, we requested information from the IRS that identifies all sensitive systems. However, our ability to obtain a complete and reliable inventory of its sensitive systems was an ongoing challenge throughout this evaluation. Our inability to readily obtain this information resulted in continued delays in our ability to complete this evaluation and report to the Chairman of the U.S. House Ways and Means Committee.

At the start of our evaluation, the IRS provided its Office of Information Technology, Cybersecurity, Architecture and Implementation function as our primary point of contact to obtain the sensitive system information we needed to perform our assessment. Management officials indicated that they did not have complete and reliable information that identifies all sensitive systems. Management officials noted that, in Fiscal Year 2022, they began an initiative to identify all IRS systems that include FTI with the goal of having the systems identified by the end of Fiscal Year 2023. Additionally, our repeated contacts with management officials requesting interim results of their identification of sensitive systems went unaddressed.

As such, we had to identify an alternate source of information we could use for our evaluation, and we elected to use information the IRS previously provided for a separate TIGTA evaluation.

Specifically, we used sensitive system information compiled by the IRS's Enterprise Security Audit Trail (ESAT) office. This information primarily identified systems that process PII, which includes FTI. The ESAT office manages the enterprise audit initiative, oversees the deployment of information technology solutions to resolve systemic audit trail issues, and monitors compliance with the requirement to ensure that complete and accurate audit trail logs are created for all sensitive systems. As of June 1, 2023, the IRS's ESAT office reported that it had identified 364 sensitive systems. In October 2023, the IRS informed us that based on its continued analysis and assessment, it reduced the number of sensitive systems to 319.

Inconsistent sensitive system naming conventions presented further challenges in performing our assessment

Once we obtained the previously mentioned information from the ESAT office, we attempted to identify the 364 sensitive systems in BEARS, which is the dataset that would enable us to identify specific users permitted access to one or more of these 364 systems. However, due to differences in the sensitive system naming conventions used by the ESAT office and what was listed in BEARS, we were unable to match 88 of the 364 sensitive systems identified by the ESAT office to systems in BEARS.

On August 1, 2023, we alerted management of our inability to identify these 88 systems in BEARS. We provided management with the list of these 88 systems and requested that they review the list and determine why BEARS data were not available for these sensitive systems. The IRS subsequently provided TIGTA with information to identify and crossmatch the 88 systems that we could not previously identify. However, this information was provided after our analysis was completed. As such, to prevent delays in our evaluation, we limited our assessment to the 276 sensitive systems identified by the ESAT office that we could match to BEARS.

The IRS's lack of a complete list of sensitive systems and not employing an enterprise-wide consistent and universal naming convention for these systems has been reported on by TIGTA. For example, in July 2022, TIGTA's Office of Audit (OA) reported that the IRS could improve on maintaining a comprehensive and accurate inventory of its information systems.[5] Most recently TIGTA issued a report in October 2023 concluding that the IRS is not effectively identifying and tracking all systems with FTI.[6] Management officials stated that they had not perfected the list at the time the previously mentioned audit was conducted. However, as of November 2023, management stated that they have a complete and validated list of the sensitive systems and are working to resolve the naming convention issue. Specifically, a consistent taxonomy (*e.g.*, a scheme of classification) is required to ensure that all systems with access to sensitive data are identified to ensure that taxpayer data are safeguarded. TIGTA recommended that the IRS direct a taxonomy reconciliation across the enterprise to standardize IRS system classification. The IRS agreed with this recommendation.

[5] TIGTA, Report No. 2022-20-040, *Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation* (July 2022).

[6] TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (Oct. 2023).

Results of Review

We identified that users are granted access to sensitive systems via the BEARS application and that the process is the same for employees and contractors. Our analysis of BEARS data as of July 13, 2023, identified 153,120 users who have or had access to one or more IRS information technology systems.[7] Of the 153,120 users, 13,231 were contractors. Specific to our evaluation of the 276 sensitive systems, our analysis of BEARS identified a total of 91,661 users, of which 5,068 were contractors, authorized to access one or more of these sensitive systems.

In addition, we identified that procedures to systemically remove users who no longer require access to sensitive systems were not always working as intended. Specifically, our assessment of the 91,661 users identified that actions were not always taken to timely remove users once they separated from the IRS. For example, we identified 279 users who were listed in BEARS as separated, who as of July 13, 2023, continued to have access to at least one IRS sensitive system. However, for each of these individuals IRS network access was removed, which according to the IRS, reduces, but does not eliminate, the risk that a user can access a sensitive system.

We also identified that the IRS did not always remove contractor access to sensitive systems when background investigations were not favorable. Internal guidelines state that contractors, unlike IRS employees, must have a background investigation with a favorable interim or final determination prior to being granted network and sensitive system access and generally must continue to maintain favorable determinations upon re-investigation.[8] Of the 5,068 users listed in BEARS as a contractor, 19 contractors' most recent background investigations were not favorable as of July 13, 2023. These contractors still retained their access to one or more sensitive systems because the IRS did not take action to suspend or disable the contractors from the IRS's systems as required.

Finally, we found that the IRS is evaluating steps to improve its ability to safeguard data housed on its sensitive systems. These steps include identifying and recording user actions when accessing sensitive data and tracking authorized and unauthorized attempts of removal of sensitive data from its systems. A key initiative is the IRS's CDW enhanced data security project. The goal of this project is to enhance security controls for user access and data exporting of FTI from RAAS systems.

However, the fact remains that for some sensitive systems, the IRS does not have adequate controls to detect or prevent the unauthorized removal of data by users. TIGTA has repeatedly reported that a key deficiency in the IRS's detection and deterrence processes is not ensuring that all sensitive systems are providing complete, accurate, and usable audit trail logs for monitoring and identifying unauthorized access and for other investigative purposes. Since 2002, TIGTA's OA has issued seven reports that detail the IRS's audit trail deficiencies with

[7] BEARS includes historical data for users (employees and contractors) who have separated from the IRS. Therefore, not all users may be actively employed by the IRS.

[8] The IRS conducts a fitness determination for new employees, which if favorable, finds the individual as suitable, or fit, to perform work for or on behalf of the Federal Government and therefore the employee is eligible to hold a sensitive position. According to IRS internal guidelines, due to the risk associated with granting access prior to the completion of the required background investigation, interim system and network access will be granted only in cases where it has been determined that the risk is acceptable.

the most recent report being issued in October 2023.[9] During our discussions relating to the results of this assessment, IRS officials informed us that they are now capturing and sending audit trail data for all of its operational sensitive applications to a centralized repository.

The IRS uses audit trail logs to monitor for unauthorized access (UNAX). While the IRS performs some upfront screening for UNAX violations, such as accessing one's own tax account and behavioral anomalies indicative of potential UNAX violations, TIGTA's Office of Investigations is responsible for investigating all potential UNAX allegations. TIGTA's investigative efforts rely on the availability of complete and accurate audit trail logs. TIGTA's Office of Investigations is still working to validate and test the newly created audit trail logs to ensure that they are complete, accurate, and usable for all systems.

The following sections provide responses to the Chairman's concern relating to access to and safeguarding of taxpayer information maintained by the IRS.

Who Has Access to Sensitive Information?

Our analysis identified that the primary users permitted access to sensitive systems are IRS employees, TIGTA employees, and contractors.[10] Additionally, the IRS indicated that certain external users can also be granted access to its sensitive systems. These external users include:

- **Joint Committee on Taxation (JCT)** – The JCT is a nonpartisan committee of the U.S. Congress. The JCT operates with an experienced professional staff of economists, attorneys, and accountants who assist Members of the majority and minority parties in both houses of Congress on tax legislation. The JCT's duties include consideration of possible changes in tax laws which can lead to their clarification, simplification, or revision to prevent undue hardships or the granting of unintended benefits.
- **Joint Statistical Research Program** – A collaborative research program, within the IRS's Statistics of Income Division, the Joint Statistical Research Program is where non-IRS researchers are granted access to IRS sensitive systems to work with Statistics of Income staff on specialized research projects benefiting tax administration.
- **U.S. Department of the Treasury, Office of Tax Analysis** – The Office of Tax Analysis analyzes the effects of the existing tax law and alternative tax programs and prepares a variety of background papers, position papers, policy memoranda, and analytical reports on economic aspects of domestic and international tax policy.
- **External Law Enforcement Personnel** – IRS Criminal Investigation works with external law enforcement individuals who are uniquely assigned to sensitive task forces or perform sensitive investigative duties. In certain cases, these law enforcement personnel are provided access to IRS sensitive systems for the express purpose of conducting investigations or providing support to task forces.

Throughout our review, the IRS was challenged in its ability to identify all sensitive systems. However, as of November 2023, IRS management stated that they have a complete and validated list of the sensitive systems. TIGTA OA's Security and Information Technology Services

[9] Appendix II provides a list of the prior TIGTA OA reports.

[10] Contractors are individuals external to the IRS that supply goods and services according to a formal contract and task order. These services may include cybersecurity and information technology consulting.

business unit conducts and plans to continue to perform audits related to the IRS's efforts to identify sensitive systems. For example, in October 2023, the OA recommended that the IRS direct taxonomy reconciliation across the enterprise to standardize the IRS's systems naming conventions to address mismatched data and ensure that the ESAT office has a complete and accurate inventory of applicable systems.[11]

How Many Individuals and Organizations Have Access to Sensitive Information?

As of July 2023, our analysis of BEARS data identified 153,120 users who currently have or had access to an IRS information technology system, of which 13,321 are contractors. Further, of these 153,120 users, 91,661 have or had access to one or more of the 276 sensitive systems included in our evaluation. Figure 1 provides a breakdown of how the IRS classifies these 91,661 users in BEARS as employees or contractors as well as by the users' employment status as active, inactive, or separated.

Figure 1: Current and Prior Users With Access to Sensitive Systems[12]

User Type	Active	Inactive	Separated	Total
Employee	86,290	26	277	86,593
Contractor	5,066	0	2	5,068
Totals	**91,356**	**26**	**279**	**91,661**

Source: TIGTA analysis of BEARS user data as of July 13, 2023.

Contractors granted access to sensitive systems

We analyzed personnel records associated with the 5,068 users classified as contractors in BEARS. The records associated with 4,979 users indicate that these contractors were employed by 187 different companies. For the remaining 89 contractors, as of August 29, 2023, personnel records show they became IRS employees and thereafter company information was no longer relevant for them. Figure 2 provides a breakdown of the top 10 companies that account for 2,844 contractors (56 percent) of the 5,068 contractors with access to one or more sensitive systems included in our evaluation.

[11] TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (Oct. 2023).

[12] For each of these individuals IRS network access was removed, which according to the IRS reduces, but does not eliminate, the risk that a user can access a sensitive system.

Figure 2: Top 10 Contracted Companies With Access to IRS Sensitive Systems

Business	Number of Contractors
Contractor A	699
Contractor B	434
Contractor C	372
Contractor D	343
Contractor E	260
Contractor F	201
Contractor G	161
Contractor H	133
Contractor I	130
Contractor J	111

Source: TIGTA analysis of BEARS user data as of July 13, 2023, and IRS Human Capital Office employment information (HRConnect) as of August 29, 2023, and October 23, 2023.

How Is Sensitive Information Accessed and for What Purpose?

Generally, every incumbent employee and contractor must undergo a suitability screening and/or background investigation.[13] A background investigation encompasses various components of an individual's personal background with verification steps that may include:

- Federal Bureau of Investigation fingerprint check.
- Credit check.
- IRS Automated Labor and Employee Relations Tracking System check.
- Federal tax compliance check.
- U.S. Citizenship check.

According to the IRS's internal guidelines, the IRS performs prescreening investigative steps (like those listed) for employees. Once an individual is onboarded as a new employee, the IRS then initiates the complete background investigation. Internal guidelines note that when feasible, all background investigations shall be completed and suitability decisions made within a new employee's first year of service.

However, contractors, unlike IRS employees, generally must have a background investigation with a favorable determination prior to being approved access to a sensitive system.[14] To maintain system access, contractors generally must continue to receive favorable determinations in subsequent background re-investigations. As of July 13, 2023, our review of background

[13] IRS Personnel Security is responsible for the adjudication of background investigations for contractor employees.

[14] Contractors may be given interim system and network access prior to the completion of a background investigation.

investigation data identified that 19 of the 5,068 contractors' most recent background determinations were not favorable, yet all 19 contractors had network and sensitive system access. According to the IRS's internal guidelines, the contractor's access to IRS systems must be immediately:

- Suspended until a final determination is made and when a proposal to either revoke interim or deny final system access letter is issued.
- Disabled when a memorandum of a final denial for system access is issued.

The IRS issued a denial of access notification to the Contracting Officer's Representative for all 19 individuals. However, IRS management informed us that the respective Contracting Officer's Representatives did not take action to suspend or disable the contractors from the IRS's systems, as required. Our tests were not designed to determine whether there were any data loss incidents related to these contractors and we made no assertions regarding this.

In November 2023, the IRS disabled network access for eight of the 19 contractors. The remaining 11 contractors who did not have a favorable background investigation as of July 13, 2023, subsequently received a favorable determination to support their access to IRS systems as of November 2023. However, the fact remains that the IRS should have suspended or disabled these contractors' access until a favorable determination was on file.

Recommendation 1: The Deputy Commissioner for Operations Support should ensure that access to sensitive systems is immediately suspended or disabled when a contractor is identified as not having a favorable background determination.

Management's Response: The IRS agreed with our recommendation and plans to 1) develop additional training for Contracting Officer's Representatives to ensure adherence to established separation procedures and timelines following negative background determinations and 2) evaluate the feasibility of automating these processes to streamline the access removal process, which would require integrating disparate IRS systems and Treasury's personnel system.

Office of Inspections and Evaluations Comment: Although the IRS agreed with this recommendation, we have a concern with the January 2026 implementation date. We believe that the IRS could implement training and evaluate the feasibility of automating these processes in a more expeditious time frame than the January 2026 implementation date.

Other concerns related to contractors who had network and system access

We identified other concerns related to contractors, as follows:

- As of July 13, 2023, three contractors did not have any active contracts with the IRS and retained their network and system access. TIGTA's OA is currently assessing the effectiveness of processes to remove contractor access to IRS facilities, systems, and equipment upon separation or transfer of duties.[15] We have referred this issue to this audit team for additional follow-up.

[15] TIGTA, Audit No. 202310026, *Review of Contractor Separation and Transfer Procedures*.

- As of July 13, 2023, 10 individuals received favorable background determinations for employment as a contractor. However, the individuals subsequently applied for Federal employment and did not receive a favorable determination to become an IRS employee. The IRS Personnel Security office stated that it reviewed the 10 individuals who were denied Federal employment and were retained or approved as IRS contractors. The IRS Personnel Security office concluded that the correct determinations were made and the results of the Federal employee background investigations did not prohibit the individuals' ability to continue employment as an IRS contractor. Although the IRS believes that these were the correct determinations, we are concerned that these individuals who were not considered suitable for IRS employment were retained as contractors and were given access to sensitive systems. We plan to evaluate this matter for additional review.

Network access is provided when a user account is activated

Generally, access to the IRS network is authorized for IRS employees once suitability screening is performed and for contractors once a favorable background investigation is completed. Employees and contractors are granted access to the IRS network when their user account is created. Once the IRS activates a user's account, the user may be provided with a username and password or other type of login (*e.g.*, Personal Identity Verification card) to access the IRS's network. The IRS also provides users with equipment (*e.g.*, computer) for use that has been authorized to access the IRS network. Finally, users must also sign a Rules of Behavior Form within a specified period of being granted access to the IRS network to maintain access and to avoid their accounts being disabled. The Rules of Behavior Form describes a user's responsibilities and expected behavior for information and system usage, security, and privacy.

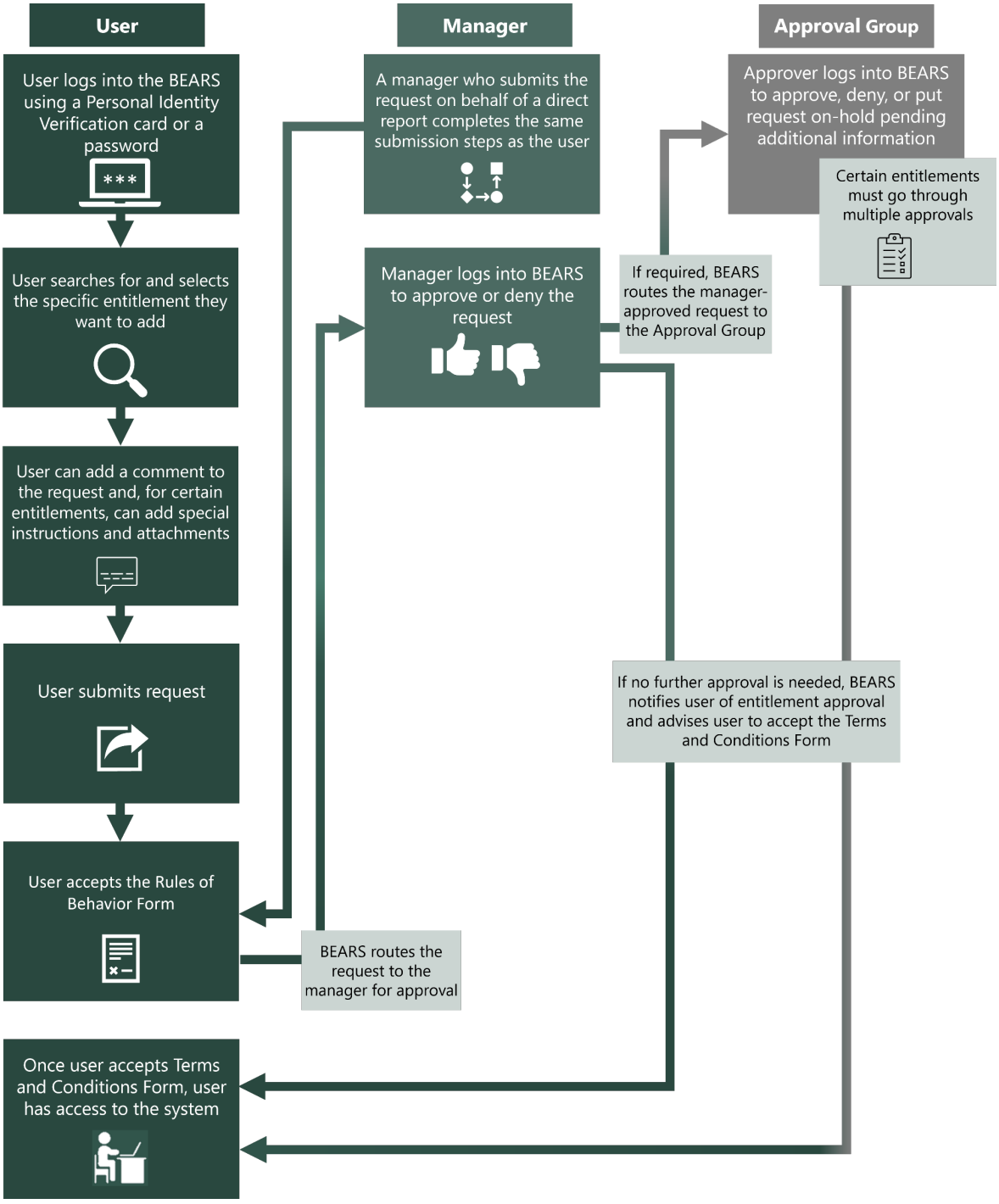
Approval Groups are ultimately responsible for approving or denying user access

As previously noted, users submit their request for access and approval to sensitive systems via BEARS. All IRS employees, TIGTA employees, contractors, and other users must request this access using BEARS. The BEARS request and approval process includes the following:

- User submits a request in BEARS to access a particular sensitive system.
- User's immediate manager approves the request in BEARS.

Once approved by the manager, the request is forwarded via BEARS to the responsible sensitive system Approval Group. The Approval Group is ultimately responsible for approving or denying user access to a sensitive system. Figure 3 provides a step-by-step overview of the BEARS request and approval process.

Figure 3: BEARS Request and Approval Process



Source: TIGTA analysis of IRS BEARS Manager and End-User Guidebooks and information from IRS officials.

Access to some sensitive systems requires a business justification

According to the IRS, access to some sensitive systems requires users to provide a written justification as to why they need to be granted access to the system. For those sensitive systems that require a written justification, the user's manager and the Approval Group are responsible for ensuring that the required written justification is included with the user's request. However,

our evaluation identified that there is no documentation outlining when a business justification is in fact needed for a user to have approved access to a sensitive system. The IRS stated that whether a business justification is required is at the sole discretion of the system's business owner or technical point of contact for the entitlement.

Procedures to systemically remove users who no longer require access to sensitive systems were not always working as intended

Our evaluation identified that not all user accesses are timely removed once they separated from the IRS. Specifically, we identified that 279 of the 91,661 users with sensitive system access were listed in BEARS as separated and continued to have access to one or more sensitive systems as of July 13, 2023. For 276 of these users, we determined that they had been separated from the IRS between six and 502 days without their systems' access being removed.[16] When we discussed our results with IRS management, they noted that they are aware of these types of situations. However, for each of these individuals IRS network access was removed, which according to the IRS, reduces, but does not eliminate, the risk that a user can access a sensitive system.

In response to management's assertion that although separated users' access to a sensitive system is not being timely removed but network access is removed, we expanded our assessment to all 153,120 users in BEARS. This resulted in our identifying an additional 20 separated users who did not have their network access removed. However, these users had their access to sensitive systems removed.

When we discussed our results with IRS management, they noted that the automated process to remove network and sensitive system access once an employee or contractor separates did not seem to work correctly for these individuals. Management stated that they would research the anomalies to identify the root cause to ensure recordation of all network access disablements. The IRS stated that a process has been established that includes a systemic integration between HRConnect and BEARS. The IRS explained that when a person's employment status changes, a personnel action is generated within the HRConnect system. Information regarding the employment status change is then systemically sent to BEARS for actions to be taken based on the nature of the personnel action. For example, if someone separates from the IRS, BEARS should automatically remove the user's network access.[17] Although other previously approved systems access for the user could remain active, the IRS stated that this is acceptable because the network access has been removed. Without network access, the employee should not be able to access any sensitive system.

Recommendation 2: The Chief Information Officer should ensure that user network access and sensitive system access are timely removed for users who separate from the IRS.

Management's Response: The IRS agreed with our recommendation. The IRS plans to ensure that all of the system-level user accounts for the 279 separated users are purged and plans to continue its ongoing effort to improve its processes for the identification and resolution of any separated user accounts that have not been timely purged.

[16] For one user identified as separated, we found no employment record in the HRConnect. Further, two users were identified in HRConnect; however, no separation date was identified.

[17] To remove the user's network access, the IRS deprovisions the user's account.

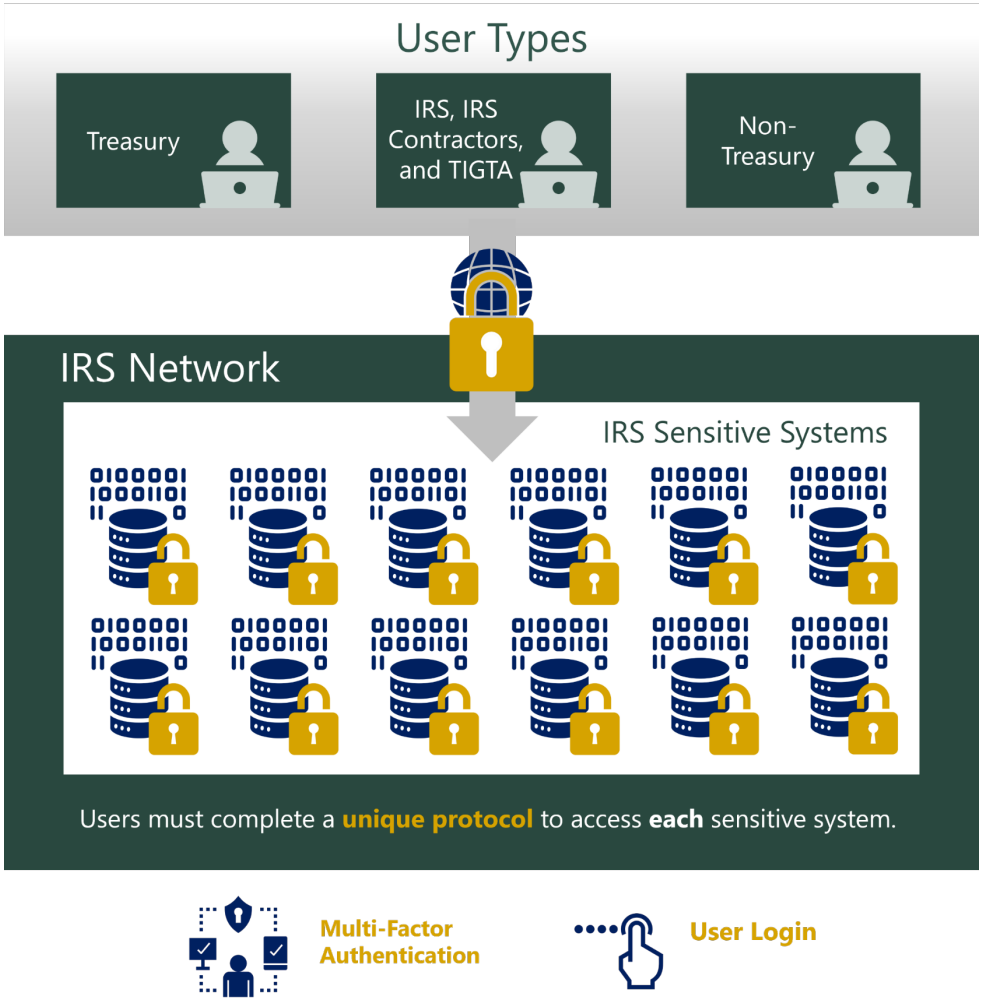
How Is Sensitive System Access Gained and How Is Sensitive Information Safeguarded?

IRS officials informed us that for a user to gain access to a sensitive system, the user must be granted both:

- **Network Access** – The ability to log on to the IRS network. As previously mentioned, users are granted access to the IRS network when their account is activated.
- **Sensitive System Access** – The ability to log on to a specific sensitive system within the IRS network.

The process to gain access to a sensitive system differs from system to system. Sensitive systems have their own separate protocols for how users access the system. For example, accessing sensitive systems may be through an application or software installed on the user's computer, or using a web-based browser with the user being required to either input a user login or complete multifactor authentication using a Personal Identity Verification card. Figure 4 provides an overview of how users access sensitive systems.

Figure 4: Access to an IRS Sensitive System Through the IRS Network



Source: TIGTA analysis of IRS's CDW Environment documentation as of August 24, 2023, analysis of BEARS user data as of July 13, 2023, and other IRS documentation.

Although management noted that for users to gain access to a sensitive system, they first need to be granted network access, we identified 1,664 users who had no evidence of any network access in BEARS but had access to at least one system. These users included 1,566 users from the IRS's Criminal Investigation and 98 from TIGTA. Based on our identification of these users, IRS management corrected their position and noted that:

- The 1,566 Criminal Investigation users were the first users who migrated to BEARS prior to the IRS establishing network access approvals. Therefore, network access approvals are not listed in some users' accounts. Individuals' network access requirements were not updated when the IRS converted these individuals to BEARS.
- For the 98 TIGTA users, the IRS does not have BEARS integration with the TIGTA-specific Local Area Network to automate the detection of which users have active or inactive TIGTA-specific Local Area Network accounts. As such, BEARS shows these users as not having IRS network access yet having access to sensitive systems.

Recommendation 3: The Chief Information Officer should ensure that the 1,566 Criminal Investigation users' network access is updated in BEARS.

Management's Response: The IRS agreed with our recommendation and will revise the BEARS recordation procedures to ensure that network access reports provided to TIGTA in the future contain the status for all Criminal Investigation users.

Efforts to safeguard FTI on sensitive systems

The IRS has implemented processes and procedures to try and safeguard FTI. For example, these processes include:

- **Establishment of a Data Loss Prevention Program** – Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Data Loss Preventions (DLP) System is an automated tool that monitors outgoing unencrypted employee e-mail (including attachments) and web traffic to attempt to identify the unencrypted sending of PII. For example, when an e-mail containing unencrypted PII is detected, the SPIIDE DLP System will block the message and prevent it from leaving the IRS boundary. The sender of the message will receive an automated message advising them that their message was blocked and delivery prevented.

  As of March 2023, IRS guidelines stated that the DLP uses the SPIIDE tool to scan unencrypted, outbound transmissions. These scans are intended to advance data protection and reduce inadvertent disclosures. TIGTA OA is planning an audit to evaluate the IRS's controls to prevent the loss or theft of sensitive taxpayer data. This audit is expected to be delivered in Fiscal Year 2024.

- **Periodic recertifications** – Managers must periodically recertify that users have a continued need for access to a sensitive system. IRS internal guidelines note that these recertifications ensure that users retain access to only the systems they need to complete their jobs. Non-privileged access users must be periodically recertified after a specified period. Whereas privileged access users will be recertified more frequently due to their level of access. According to the IRS, recertification is a key control to protecting IRS data and systems from threats and helps maintain the security of IRS networks. IRS management stated that the recertification process is automated and monitored for compliance by IRS Cybersecurity.

As we noted previously in our report, the IRS initiated the CDW enhanced data security project to improve security controls for user access and monitor FTI data obtained from the CDW. As of August 2023, IRS management noted that this project has five major focus areas:[18]

- **Evidence Logging** – Create an evidentiary copy of all data queried within the CDW that contains PII and FTI for further analysis related to the unauthorized access, attempted access, and inspection of taxpayer records.

[18] A firewall boundary around all RAAS systems to enable an evidentiary copy of all data extracted, centralize analysis and data storage, direct limited data exports to one location/drive, apply a permanent sensitivity label to the data, and block file sharing outside the IRS network.

- **Reduce Desktop Analytics** – Provide the required tools to perform data analytics within RAAS sensitive systems to reduce the need to export data for analysis on desktop analytic tools.
- **Control Data Exports** – Enforce an approved destination for data exports and disable the ability to copy those files to unapproved drives/folders.

  According to the IRS, users associated with the JCT will continue to be permitted to remove sensitive data from the IRS environment with no visibility on the part of IRS as to what occurs when this sensitive data are removed.
- **Apply Sensitivity Labels** – Assign a high-security sensitivity label to all files with data originating from RAAS sensitive systems.
  - IRS management noted they are in the process of gathering data from RAAS environment users to identify their specific needs (*e.g.*, use cases) when accessing RAAS environment. Management noted that the identification of the individual use cases is intended to help better understand data use patterns and to determine what additional layers of security can be added without creating a work stoppage. As of August 2023, the IRS has identified over 115 CDW use cases.
- **Block External Sharing** – Block data originating from RAAS sensitive systems from leaving the IRS, as appropriate (*e.g.*, removable media/e-mail).

As of August 2023, the IRS stated that it continues to make progress on advancing these goals. However, IRS officials noted that they do not have a final completion date because the work will be perpetual given the quickly evolving technology landscape. IRS management noted that, based on the success of this project, additional sensitive systems will be identified to apply the same safeguards. In addition, IRS management also noted they are in the process of:

- Moving sensitive system users to a cloud environment, which will allow the IRS to better monitor user access to data.
- Exploring options for implementing Digital Rights Management to allow management to grant specific privileges/functions to users as well as prohibit specific privileges and functions when accessing a sensitive system. For example, if the use of removable media with read and write access is systematically blocked and a specific user needs removable media with read and write access to perform work duties, Digital Rights Management can be used to grant the user permission. The IRS is evaluating the use of Digital Rights Management to limit user access to data and the ability to remove these data.

Finally, management noted that the additional funding it has been provided under the Inflation Reduction Act of 2022 has enabled the IRS to take actions to improve the safeguarding of FTI.[19] However, the loss or decrease in this additional funding will impact its ability to timely develop additional information technology improvements. Specifically, when information technology funding through normal appropriations is reduced, the IRS can rely on the separate funding from the Inflation Reduction Act of 2022. Should this funding also be reduced, the IRS will have to reassess its efforts to address numerous information technology deficiencies and planned improvements.

[19] Public Law No. 117-169, 136 Stat. 1818.

Concerns remain regarding the IRS's ability to adequately safeguard FTI stored in sensitive systems as well as detect unauthorized accesses to this data

Although the IRS is evaluating the actions previously discussed to improve its ability to safeguard data on its sensitive systems, the fact remains that for some sensitive systems the IRS does not have adequate controls to detect or prevent the unauthorized removal of data by users. TIGTA has repeatedly reported that a key deficiency in the IRS's detection and deterrence processes is not ensuring that all sensitive systems are providing complete, accurate, and usable audit trail logs for monitoring and identifying unauthorized access and for other investigative purposes. Since 2002, TIGTA has issued seven reports that detail the IRS's audit trail deficiencies with the most recent report being issued in October 2023. During our discussions relating to the results of this assessment, IRS officials informed us that they are now capturing and sending audit trail data for all of its operational sensitive applications to a centralized repository.

IRS employees, including contractors, are only authorized to access tax information when it is required for official IRS tax administration duties. UNAX occurs when an IRS employee accesses tax information that is unnecessary to the performance of their assigned duties or is otherwise prohibited. The willful unauthorized access or inspection of taxpayer records is a crime punishable upon conviction by fines, prison terms, and termination of employment.

The IRS uses audit trail logs to monitor for UNAX. While the IRS performs some upfront screening for UNAX violations, such as accessing one's own tax account and behavioral anomalies indicative of potential UNAX violations, TIGTA's Office of Investigations is responsible for investigating all potential UNAX allegations. TIGTA's investigative efforts rely on the availability of complete and accurate audit trail logs. TIGTA's Office of Investigations is still working to validate and test the newly created audit trail logs to ensure that they are complete, accurate, and usable for all systems.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this evaluation was to assess user access to taxpayer information maintained by the IRS and identify the number of IRS systems that contain taxpayer information. To accomplish this evaluation, we:

- Identified and assessed the process by which IRS information systems containing taxpayer information are accessed and managed, and, to the extent possible, for what purposes.
- Determined what persons or entities have access to IRS systems containing taxpayer information (*e.g.*, IRS employees, contractors, researchers, other Federal and State Government agencies and employees).
- Discussed with key IRS officials the IRS's plans to develop and implement a process to ensure that taxpayer data are accessible only within the IRS computing environment.
- Determined whether contractors with access to taxpayer information maintained by the IRS were properly screened and investigated prior to access to sensitive systems and information being provided.

Performance of This Review

This review was performed with information obtained from IRS Human Capital and Information Technology located in Washington, D.C., during the period May through November 2023. We conducted this evaluation in accordance with the Council of the Inspectors General for Integrity and Efficiency Quality Standards for Inspection and Evaluation.

Major contributors to the report were James A. Douglas, Director; Frank J. O'Connor, Director; John L. da Cruz, Supervisory Evaluator; Taylor C. McDonald, Lead Evaluator; Malissa A. Livingston, Senior Auditor; Angelica D. Garred, Auditor; and Isaac A. Huaman, Evaluator.

Data Validation Methodology

We performed tests to assess the reliability of data from BEARS, the Automated Background Investigations System, the Treasury Human Capital Office HRConnect system, and the TIGTA Data Center Warehouse. 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.

Appendix II

Prior TIGTA Reports on IRS Audit Trail Deficiencies

March 2002
User Activity on Most Sensitive Computer Systems Is Not Monitored
Report No. 2002-20-075

The IRS did not routinely review audit trails for its networks and over 250 sensitive systems except for the Integrated Data Retrieval System. In addition, the IRS did not ensure that: sufficient capacity exists to run audit trails, automated audit reporting tools were procured to assist in evaluating audit trails, personnel have been assigned to review audit trails, and guidance on how to review audit trail reports had been developed.

August 2004
The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning
Report No. 2004-20-135

In November 2002, the IRS primary Modernization contractor delivered the Security Audit and Analysis Systems to gather audit trail information from IRS systems and store this information in a central database that IRS management, incident response teams, and TIGTA investigators could access. However, software performance and functionality problems with the system have prevented users from accessing audit trail data.

September 2004
The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness
Report No. 2004-20-131

While the IRS developed an enterprise-wide audit trail strategy to ensure review of audit trails data are conducted on a routine basis, TIGTA found that: some servers cannot generate audit trails without impairment to the server's performance, audit trails on applications have not been addressed, and modernized systems to collect and generate useful audit trail reports were not working as intended.

September 2012
Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data
Report No. 2012-20-099

TIGTA found process improvements were needed to ensure audit trails effectively support UNAX investigations and the IRS's ability to identify noncompliant activity and to hold employees accountable for UNAX policies. Specifically, audit trail logs did not include all events and data elements, and audit trail log data were not sufficiently tested and validated to ensure their accuracy and completeness.

September 2015
Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected
Report No. 2015-20-088

TIGTA found that not all systems in development had audit trail requirements adequately assessed prior to deployment, and those that did address the requirements, were not properly transmitting audit trail data after deployed. In addition, system owners were not timely documenting and tracking these audit trail deficiencies for remediation, so the deficiencies could persist indefinitely.

July 2020
Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information
Report No. 2020-20-033

The IRS continued to have challenges with ensuring that all applications are providing complete and accurate audit trails for monitoring and identifying unauthorized access and for other investigative purposes. Specifically, the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and PII and not all applications with audit trail deficiencies were being tracked and monitored as required.

October 2023
The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement
Report No. 2024-200-005

TIGTA determined that the IRS had not fully implemented its automated tool for monitoring event logging requirements as required by the Office of Management and Budget. In addition, the IRS was not sending event log data (*i.e.,* audit trail data) for 125 (35 percent) of 356 systems to the data repository for the detection and investigation of unauthorized accesses of PII and FTI.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

January 19, 2024

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL
FOR INSPECTIONS AND EVALUATIONS

FROM: Melanie R. Krause
Acting Deputy Commissioner for Operations Support

Melanie R. Krause Digitally signed by Melanie R. Krause Date: 2024.01.19 17:01:17 -05'00'

SUBJECT: Draft Audit Report – Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information (Engagement # IE-23-026)

Thank you for the opportunity to respond to this report. We deeply appreciate TIGTA's continued partnership in addressing the critically important issue of safeguarding federal tax information.

During the past year, the IRS has strengthened our internal systems, protocols and procedures by implementing numerous improvements. These include more robust data encryption, stronger 24/7 monitoring that improves insight into suspicious activity on the IRS network, and expanded audit trails that improve the surveillance of internal and external accesses to IRS sensitive systems. With the critical investments made possible by multi-year Inflation Reduction Act funding, our cybersecurity modernization efforts have made important progress in these and other areas. This has helped improve our overall security posture. But it is critical that we rigorously evaluate our systems, identify vulnerabilities in our processes and continuously improve to protect the sensitive information of taxpayers. TIGTA's analysis and review is invaluable in further advancing our work to protect taxpayers and the tax system.

The ongoing IRS modernization effort to make improvements for taxpayers and tax administration includes continued investment in a highly effective and multi-layered cybersecurity program. As you previously reported, this has included deployment of the Business Entitlement Access Request System (BEARS), a DHS-recommended solution. BEARS replaced the IRS's 20-year-old entitlement management system, eliminating more than 2.2 million lines of custom computer code and enabling the IRS to fully integrate with the Department of the Treasury's identity management system.

With respect to this review, while the IRS agrees with TIGTA's recommendations, there are four areas where we respectfully submit that TIGTA's report does not accurately characterize the IRS's current security posture.

First, while the IRS agrees that we can make process improvements, we disagree with any inference that the 19 contractors TIGTA identified compromised sensitive information. The IRS already takes steps to remove access when a contractor is identified as not having a favorable background determination. Specifically, IRS Personnel Security Specialists notify the Contracting Officer's Representative (COR) on receipt of an unfavorable background determination and explicitly instruct the COR to suspend or separate the contractor in the personnel system, which triggers automated removal of network access and disablement of entitlements in BEARS. However, TIGTA reports that the IRS did not take timely action to suspend or disable network access for 19 contractors who had unfavorable background investigations. All 19 contractors received prior favorable background investigations, and 15 contractors were reinstated after resubmitting their documentation. The remaining 4 contractors had their network access disabled and have been separated in the personnel system. IRS Cybersecurity personnel confirmed that after the unfavorable background investigation, no data loss incidents occurred for these 4 contractors. To strengthen our processes, we are currently developing additional training for CORs to ensure adherence to established separation procedures and timelines following negative background determinations. Further, we are evaluating automation opportunities, which should streamline the access removal process.

Second, the IRS disagrees that separated users without network access, including the 20 users identified in the report, present a security threat as suggested by the report. IRS demonstrated that our network protections prevent any separated user from gaining access to our sensitive systems. TIGTA evaluated 153,120 BEARS users and identified 20 separated users who appeared to have network access on July 13, 2023. The IRS acknowledges that the data provided from the new BEARS system on July 13, 2023, incorrectly identified these 20 separated users as having active network access. The automated process includes sending disablement receipts to BEARS. In these rare instances (20 of the 153,120 users), BEARS did not properly record the receipt, requiring the IRS to manually confirm successful disablement. IRS provided that manual confirmation to TIGTA. In September 2022, the IRS fully implemented automated removal of user network access for employees and contractors separated in the IRS personnel system.

Further, for system level user accounts, TIGTA evaluated 2,448,783 user accounts as of July 13, 2023, and correctly noted that 279 user accounts were not timely purged, which the IRS determined was due to some IRS systems' reliance on manual processes to purge user accounts. Without continued access to the IRS network, however, these users could not access sensitive IRS systems. IRS has an ongoing effort to automate the purging of user accounts at the system level, eliminating the need for manual actions by systems administrators. Although network access is a necessary prerequisite to access IRS systems, this automation will remove inaccessible user accounts and record those disablements in BEARS more timely.

Third, TIGTA asserts that removing network access "reduces, but does not eliminate, the risk that a user can access a sensitive system." This phrasing does not reflect the

IRS's position but rather a hypothetical posed during a telephone call with TIGTA, which was immediately challenged by IRS Cybersecurity leadership. Further, TIGTA's audit did not identify any instance of a separated user either attempting or gaining access to a sensitive system after disablement of their network access. Accordingly, characterizations predicated on hypothetical risks are potentially misleading. The IRS is confident that removing network access does eliminate the risk that a separated user can access a sensitive system. Nevertheless, the IRS has an ongoing effort to improve our processes for the identification and resolution of any separated user accounts that have not been timely purged.

Fourth, the IRS disagrees with TIGTA's finding that BEARS does not contain evidence of network access for 1,566 Criminal Investigation users. The IRS demonstrated that automated provisioning and deprovisioning of network access has been implemented for Criminal Investigation users. However, the status for these users required producing additional BEARS reports. Therefore, we have agreed with TIGTA's recommendation and will revise the BEARS recordation procedures to ensure that network access reports provided to TIGTA in the future contain the status for all Criminal Investigation users.

Collectively, IRS's security improvements have made the tax system more effective, efficient and secure as we adapt and respond to the many evolving threats to taxpayer data and the trillions of dollars that flow through the IRS each year. The IRS has also strengthened data protections through accelerating implementation of corrective actions to address dozens of security-related recommendations and will continue to focus on strengthening our security and privacy controls. Continuous improvement is the cornerstone of all IRS data security programs. We appreciate your recommendations and have attached our corrective action plan.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact Kaschit Pandya, Acting Chief Information Officer, at 202-317-5000.

Attachment

Evaluation # IE-23-026, Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information

RECOMMENDATION 1: The Deputy Commissioner for Operations Support should ensure that access to sensitive systems is immediately suspended or disabled when a contractor is identified as not having a favorable background determination.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The IRS already takes steps to respond and remove access when a contractor is identified as not having a favorable background determination. Specifically, IRS HCO Personnel Security Specialists notify the Contracting Officer's Representative (COR) on receipt of an unfavorable background determination. The COR must then follow separation procedures and initiate separation actions in the personnel system, which triggers automated removal of network access and disablement of entitlements in BEARS. To strengthen our processes, we are currently developing additional training for CORs to ensure adherence to established separation procedures and timelines following negative background determinations, and we are evaluating the feasibility of automating these processes to streamline the access removal process, which would require integrating disparate IRS systems and Treasury's personnel system.

IMPLEMENTATION DATE: January 15, 2026

RESPONSIBLE OFFICIAL(S): Chief Human Capital Officer in partnership with the Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should ensure that user network access and sensitive system access is timely removed for users who separate from the IRS.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The IRS has already disabled the network access for the 279 separated users identified by TIGTA and will ensure that all of their system level user accounts are purged. Without continued access to the IRS network, these 279 users could not access sensitive IRS systems. Since September 2022, the IRS has fully implemented automated removal of user network access for employees and contractors separated in the IRS personnel system. The IRS has an ongoing effort to improve our processes for the identification and resolution of any separated user accounts that have not been timely purged.

IMPLEMENTATION DATE: January 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer for Cybersecurity

RECOMMENDATION 3: The Chief Information Officer should ensure that the 1,566 Criminal Investigation users' network access is updated in BEARS.

Attachment

Evaluation # IE-23-026, Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The IRS will ensure that the 1,566 Criminal Investigation users' network access is updated in BEARS. While the automated provisioning and deprovisioning of network access has been implemented, the status for these users required producing additional BEARS reports. Therefore, we will revise the BEARS recordation procedures to ensure that network access reports provided to TIGTA in the future contain the status for all Criminal Investigation users.

IMPLEMENTATION DATE: September 30, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Appendix IV

Office of Inspections and Evaluations Comments on Management's Response

In response to our draft report, the IRS agreed to all three recommendations, but disagreed with TIGTA's characterization of the IRS's "current security posture." Our report provides an analysis of the security posture at the time our review. The following text includes portions of management's response and our related comments.

Management's Response: The IRS disagreed with any inference that the 19 contractors TIGTA identified compromised sensitive information. All 19 contractors received prior favorable background investigations, and 15 contractors were reinstated after resubmitting their documentation. The remaining four contractors had their network access disabled and have been separated in the personnel system. IRS Cybersecurity personnel confirmed that after the unfavorable background investigation, no data loss incidents occurred for these four contractors.

> **Office of Inspections and Evaluations Comment:** TIGTA did not make this inference, it is based on our review of IRS BEARS data. In fact, in our discussions with IRS management during our evaluation relative to these 19 contractors, they noted that the respective Contracting Officer's Representatives did not take action to suspend or disable the contractors from the IRS's systems, as required. Specifically:
>
> - For their most recent background investigation when we performed our analysis, each of these 19 contractors received an unfavorable background determination.
> - IRS internal guidelines require the contractor's access to IRS systems be immediately suspended until a final determination is made and when a proposal to either revoke interim or deny final system access, a letter is issued. This was not done. As such, these contractors continued to have access to sensitive systems.
>
> Finally, our tests were not designed to determine whether there were any data loss incidents and we made no assertions regarding this. We added a clarifying statement to the report to address this concern.

Management's Response: The IRS disagreed that separated users without network access, including the 20 users identified in the report, present a security threat as suggested by the report. The IRS acknowledged that the data provided from the new BEARS on July 13, 2023, incorrectly identified these 20 separated users as having active network access. The automated process includes sending disablement receipts to BEARS. In these rare instances (20 of the 153,120 users), BEARS did not properly record the receipt, requiring the IRS to manually confirm successful disablement. The IRS provided that manual confirmation to TIGTA. In September 2022, the IRS fully implemented automated removal of user network access for employees and contractors separated in the IRS personnel system.

Further, for system level user accounts, TIGTA evaluated 2,448,783 user accounts as of July 13, 2023, and correctly noted that 279 user accounts were not timely purged, which the IRS

determined was due to some IRS systems' reliance on manual processes to purge user accounts. Without continued access to the IRS network, however, these users could not access sensitive IRS systems.

> **Office of Inspections and Evaluations Comment:** Subsequent to the issuance of the draft report, the IRS provided information to support that the 20 separated users did in fact have their network access timely removed, despite BEARS data not accurately reflecting the users' network access status. However, management did not provide our office with information documenting why BEARS data were inaccurate.
>
> The IRS asserts that in its response that there is no risk when users continue to have sensitive systems access when the network access has been removed. While the existing timely and systemic disabling of separated users' network access mitigates the risk that a user could potentially access a sensitive system, we do not agree that this risk is completely eliminated.

Management's Response: TIGTA asserts that removing network access "reduces, but does not eliminate, the risk that a user can access a sensitive system." This phrasing does not reflect the IRS's position but rather a hypothetical posed during a telephone call with TIGTA, which was immediately challenged by IRS Cybersecurity leadership. Further, TIGTA's audit did not identify any instance of a separated user either attempting or gaining access to a sensitive system after disablement of their network access. Accordingly, characterizations predicated on hypothetical risks are potentially misleading. The IRS is confident that removing network access does eliminate the risk that a separated user can access a sensitive system.

> **Office of Inspections and Evaluations Comment:** While the IRS believes that there is no risk that a separated user can access sensitive systems without network access, we cannot say the risk is completely eliminated. While we agree that the risk is mitigated, we believe that there is a potential risk. Further, IRS actions to timely remove user accounts for separated users, regardless of network access status, indicates a perceived risk does exist.

Management's Response: The IRS disagreed with TIGTA's finding that BEARS does not contain evidence of network access for 1,566 Criminal Investigation users. The IRS demonstrated that automated provisioning and deprovisioning of network access has been implemented for Criminal Investigation users. However, the status for these users required producing additional BEARS reports.

> **Office of Inspections and Evaluations Comment:** At the time we conducted our analysis, BEARS data, as we reported, did not accurately reflect the network access status for IRS Criminal Investigation users. Subsequent to bringing this matter to the IRS's attention, the IRS noted that it is taking actions to address the accuracy of BEARS data to reflect Criminal Investigation users' network access status.

Appendix V

Glossary of Terms

Term	Definition
Applications	An information technology component of a system that utilizes information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
Audit Trail Log	Records of actions performed by individuals who access an IRS system. All IRS sensitive systems are required to have an audit trail log.
Automated Labor and Employee Relations Tracking System	An application used to track labor and employee relations case data. It was developed to ensure consistency in tracking labor and employee relations disciplinary actions.
Business Entitlements Access Request Systems	A means to request and document user access to systems/applications.
Compliance Data Warehouse	The IRS's primary research information system that includes a wide array of sensitive information. It provides a single integrated environment of data and computing services to support the research and analysis needs of IRS employees and contractors.
Deprovision	The process by which access rights to software and network services are taken away; typically occurs when an employee leaves a company or changes roles within the organization.
Enterprise Security Audit Trail Office	Office that manages the enterprise audit initiative, oversees the deployment of information technology solutions to resolve systemic audit trail issues, and monitors compliance with the requirement to ensure that complete and accurate audit trail logs are created for all sensitive systems.
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.
HRConnect	A human resource system owned and operated by the U.S. Department of the Treasury.
Joint Committee on Taxation	A nonpartisan committee of the U.S. Congress. The JCT's duties are set forth in Internal Revenue Code § 8022, which include consideration of possible changes in the tax laws leading to their clarification, simplification, or revision to prevent undue hardships or the granting of unintended benefits.
Joint Statistical Research Program	A part of Statistics of Income, which is a division of the IRS's Research, Applied Analytics, and Statistics office, that seeks to enable the use of tax microdata by qualified researchers outside the Federal Government.
Multifactor Authentication	A layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

Term	Definition
Non-Privileged Access	Access to a server via an application, or an application's graphical user interface, which does not login to the operating systems level is not considered privileged access.
Office of Tax Analysis	Analyzes the effects of the existing tax law and alternative tax programs and prepares a variety of background papers, position papers, policy memoranda, and analytical reports on economic aspects of domestic and international tax policy.
Online 5081	Designed to replace the paper Form 5081, *Information System User Registration/Change Request*. The application streamlined the request process for adding authorized IRS employees, vendors, and contractors as users on IRS computer systems and applications. The IRS retired this application on January 31, 2023.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of PII are name, Social Security Number, date of birth, place of birth, address, and biometric record. PII can include FTI.
Privileged Access	Defined by management as any access which logs into the operating systems level of the server including read only access.
Removable Media	Any storage device that can be removed from a computer while the system is still running. Examples include CDs, DVDs, diskettes, and USB drives.
Research, Applied Analytics, and Statistics	The IRS's centralized research and analytic organization that partners with embedded research functions to share information and analytic techniques, to collaborate on projects and identify learning and training opportunities.
Systems	A set of related components and events that interact with each other to accomplish a task.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.
User (Active)	User's employment status in HRConnect marked as "active."
User (Inactive)	User's employment status in HRConnect listed as "leave of absence," "leave with pay," "suspended," or "short work break."
User (Separated)	User's employment status in HRConnect listed as "deceased," "retired with pay," "retired," "terminated," "terminated with pay," or "terminated pension pay out."

Appendix VI

Abbreviations

BEARS	Business Entitlement Access Request System
CDW	Compliance Data Warehouse
DLP	Data Loss Preventions
ESAT	Enterprise Security Audit Trail
FTI	Federal Tax Information
IRS	Internal Revenue Service
JCT	Joint Committee on Taxation
OA	Office of Audit
PII	Personally Identifiable Information
RAAS	Research, Applied Analytics and Statistics
SPIIDE	Safeguarding Personally Identifiable Information Data Extracts
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access

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

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

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