TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform

May 28, 2026

Report Number: 2026-208-026

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

HIGHLIGHTS: The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform

Final Audit Report issued on May 28, 2026 **Report Number 2026-208-026**

Why TIGTA Did This Audit

The Enterprise Data Platform (hereafter referred to as the platform) was deployed in April 2022 to help the IRS improve the storage and management of data to support improved taxpayer services and enforcement. The platform is a cloud-based system that will provide data to IRS users and systems.

The platform securely contains authoritative data to enable reporting, analytics, customer service, application development and external sharing where appropriate.

The IRS spent approximately $178.4 million on the platform from Fiscal Year (FY) 2023 through FY 2025. We assessed the platform data migration, capabilities and security.

Impact on Tax Administration

The platform will improve operations and the customer service experience. For example, it will deliver comprehensive taxpayer account data in near-real time by creating a 360-degree view of taxpayer data to allow employees to provide improved service. The platform will also support new analytic models, such as compliance risk analytics, to improve case selection.

In addition, the platform will bring together taxpayer account, case, and operational data in a platform accessible to appropriate employees and applications, subject to controls and protections to help ensure security and privacy.

What TIGTA Found

As of December 2025, there are 46 datasets ingested onto the platform. The team ingested 37 (63 percent) of the 59 datasets from the roadmap onto the platform and 9 additional datasets that were not documented in the roadmap. The platform team expects to ingest the remaining 22 (37 percent) datasets by the end of FY 2026. While the revisions to the platform roadmap were necessary to meet business needs, they could have unintended consequences that could delay project completion.

Integration issues impact the IRS's ability to manage user access. For example, the IRS is unable to use the Privileged User Management Access System to manage the platform's privileged accounts. A privileged account means that users have elevated access and can perform actions beyond those of a standard user, *e.g.*, modify system settings, install software, *etc.* The platform has 14 approved privileged user accounts, but none are managed by the Privileged User Management Access System as required by the IRS's policy.

In addition, the IRS was unable to provide us with any evidence that these monitoring activities occurred for privileged user accounts. We identified one privileged user account without approved access that logged into the platform. This unauthorized login occurred because of an administrative error in the manual approval process.

We also identified [redacted] users that had access to the platform after their required entitlements were removed. [redacted] of these users logged into the platform and had access to datasets that contain taxpayer data. The platform team also identified the [redacted] users during their user account review and immediately took action to remove their access. By not properly managing user access, the IRS cannot ensure that only appropriate users have access to sensitive data.

Finally, the platform does not use systemic processes, *i.e.*, automated emails, alerts, *etc.*, to manage user access. It was originally scheduled to be completed by the third quarter of FY 2025. However, automation could not be achieved due to an infrastructure issue between IRS and Treasury Department networks. Despite initially identifying this risk in January 2024, it remains unresolved.

What TIGTA Recommended

We made four recommendations to improve the access controls to the platform, including that the IRS work with the Treasury Department to ensure that privileged platform user accounts are fully integrated with the Privileged User Management Access System and that the platform management team is timely notified to remove user access when appropriate.

The IRS agreed with all four of our recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

May 28, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform (Audit No.: 2025208016)

This report presents the results of our review to assess the Enterprise Data Platform's data migration, capabilities, and security. This review is part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Modernizing Information Technology.*

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

Table of Contents

Background

One of the objectives of the Internal Revenue Service's (IRS) Inflation Reduction Act Strategic Operating Plan is to deliver cutting-edge technology, data, and analytics to operate more effectively. The Enterprise Data Platform (hereafter referred to as the platform) was deployed in April 2022 to help the IRS address its data challenges. Key challenges identified by the IRS included:

- Lack of a single authoritative data source across the tax processing lifecycle.
- Lack of leading-edge analytical tools and services.
- Limited agility in delivering data solutions.
- Lack of enterprise-wide data security policies for data access.
- Limited data exchange capabilities across legacy and modern systems.
- Siloed legacy reporting solutions that consume resources needed for modernization.

The platform is a cloud-based system that will deliver universal data access for users and systems in the enterprise.[1] The platform is designed to have authoritative data on a secure platform to enable reporting, analytics, customer service, application development and external sharing where appropriate. In addition, the platform will elevate data use at the IRS by ingesting, storing, managing, and providing secure access to taxpayer and business data. The IRS spent approximately $178.4 million on the platform from Fiscal Year (FY) 2023 through FY 2025.

Improved Taxpayer Experience

The IRS's system limitations prevent taxpayers and IRS employees who provide customer service from gaining a 360-degree view of the latest information about a taxpayer's interactions with the IRS across workstreams and functions. However, the platform could help the IRS improve operations and provide new tools throughout the taxpayer and customer services experience. For example, the platform will deliver comprehensive taxpayer account data in near-real time by creating a 360-degree view of taxpayer data to allow employees to provide improved service. In addition, the platform will support new analytic models, such as compliance risk analytics, to improve case selection.

Further, a common platform for managing taxpayer interactions will also improve the consistency of the taxpayer experience while helping IRS employees assist and resolve issues for taxpayers more efficiently. A common platform for case management will standardize both the technology and the business processes used to address taxpayer-related cases across all workstreams.

Security and Privacy of Taxpayer Data

The platform will bring together taxpayer account, case, and operational data in a platform accessible to appropriate employees and applications, subject to controls and protections to help ensure security and privacy. The key projects to help achieve this goal include:

[1] See Appendix III for a glossary of terms

- **Continuing to implement best practices in cybersecurity.** This includes implementing industry and federal best practices in cybersecurity, *e.g.*, network security, identity and access management, vulnerability and threat management, and zero-trust architecture.
- **Continuing to ensure best practices in insider threat protections.** This includes continuing to implement and strengthen controls that limit access to authorized personnel for authorized purposes. In addition, expanding on internal monitoring and audit logging of all activities regarding taxpayer information or other personally identifiable information.
- **Enhancing Digital Identity Management.** This includes continuing to expand and ensure the Secure Access Digital Identity platform's effectiveness with new system and processes.

Enterprise Data Platform user access

The platform is hosted on the Department of the Treasury's Workplace Community Cloud (hereafter referred to as the Treasury Cloud). Users can obtain access to the platform in two different ways, either through the Treasury Cloud or through the Business Entitlement Access Request System (BEARS). The Treasury Department manages user access to the cloud independently through its own access management process separate from the IRS. The IRS's platform team uses BEARS to control access to the platform. BEARS is used to request, modify, and remove access for active users to IRS systems by managing the digital identity of individuals, roles, resources, and entitlements granted or removed. An entitlement is the type of access or permission a user has when logging into an application.

The IRS uses the Privileged User Management Access System (PUMAS) to manage privileged accounts on the platform, *i.e.*, users who need elevated access to the platform. Users with elevated access can perform actions beyond those of a standard user, allowing them to modify system settings, install software, *etc*. The PUMAS provides audit trails, consisting of logs and optional session recordings of all administrator actions to ensure that higher levels of security and auditability of all administrative actions that require elevated privileges.

Results of Review

Status of Data Ingestion

The IRS developed the Enterprise Data Platform Roadmap (hereafter referred to as the roadmap) to plan and prioritize datasets for ingestion onto the platform. The roadmap reflects the planned delivery approach at a point in time. However, it was revised six times from FY 2023 through FY 2025. Each revision reflected changes to priorities or business needs and delivery timelines shifted accordingly.

The IRS selected 59 datasets to ingest onto the platform. These datasets were identified based on requests from the business units and the platform team's knowledge of the IRS environment. As of December 2025, there are 46 datasets ingested onto the platform. The team ingested 37 (63 percent) of the 59 datasets from the roadmap onto the platform and 9 additional datasets that were not documented in the roadmap. The platform team expects to ingest the remaining 22 (37 percent) datasets by the end of FY 2026.

Our review of each version of the roadmap identified:

- 21 datasets that were approved and subsequently removed from the roadmap. According to platform management, the datasets were removed because the business unit did not satisfy all required ingestion steps or the business unit's priorities changed.
- Nine additional datasets that were not planned or part of the 59 datasets selected were ingested onto the platform without being documented on the roadmap.

While the revisions to the roadmap were necessary to meet business needs, they could have unintended consequences that could delay project completion.

The IRS Cannot Effectively Manage User Access Until Integration Issues Are Resolved

Agency security policies require all applications and platforms to use the PUMAS to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities *e.g.*, network and system administrators. However, we found:

- **PUMAS is not being used to manage the Enterprise Data Platform privileged accounts.** The platform has 14 approved privileged user accounts, but none are managed by the PUMAS as required by the IRS's policy. This means that the platform user accounts with elevated access rights do not have enhanced security oversight. According to the platform management team, the PUMAS cannot be integrated with the platform to manage, control, and monitor all activities associated with these privileged user accounts. The platform management team identified this as an issue and created a Plan of Action and Milestones (POA&M) in January 2024. However, the IRS has not taken any action to address this deficiency because the IRS and the Treasury Cloud maintain separate active directory environments. An active directory environment contains critical information about a user's entitlement, *i.e.*, what they are allowed to access. The PUMAS does not have the capability to manage users and service accounts external to the IRS network (active directory), such as Treasury Cloud where it is hosted.
- **No evidence that the Enterprise Data Platform privileged account activity was being monitored.** According to the platform team, the Treasury Shared Services Security Operations Center monitors privileged user accounts on the Treasury Cloud. However, the IRS was unable to provide us with any evidence that these monitoring activities occurred. Further, we identified one privileged user account without approved access that logged into the platform. This unauthorized login occurred because of an administrative error in the manual approval process. To mitigate this situation from recurring, the IRS's Enterprise Security Audit Trails team implemented a dashboard in October 2025 so the Counter Insider Threat Operations organization can monitor the platform privileged user account activity.

Lack of monitoring of privileged accounts and access can lead to outdated, misused, and stolen credentials. Further, failing to fully integrate the platform with PUMAS may lead to exploitation of security safeguards leading to unauthorized access and critical system compromise.

Recommendation 1: The Chief Information Officer should work with the Treasury Department to ensure that privileged Enterprise Data Platform user accounts are fully integrated with the PUMAS.

Management's Response: The IRS agreed with this recommendation and will work with the Treasury Department to ensure that privileged Enterprise Data Platform user accounts are fully integrated with the PUMAS.

Ineffective user account management

As previously mentioned, the platform is hosted on the Treasury Cloud. However, a lack of integration between the Treasury Cloud and the platform presents additional challenges to effectively monitor user access. For example, changes or updates to user access made on the Treasury Cloud would not be automatically reflected in the platform. We found that [redacted] platform users without the required approvals logged into the platform with access to datasets that contain taxpayer data. In addition, inactive user accounts were not deactivated or disabled as required. Specifically, we found:

- **Platform users had access to taxpayer data after entitlements were removed.** We identified [redacted] users that had access to the platform after the required entitlements were removed in BEARS. Further review of these users identified login activity for [redacted] of the [redacted] users, while the remaining [redacted] users did not log into the platform. These [redacted] users had access to 38 different datasets within the platform, such as the Customer Account Data Engine 2, which contains more than 360 million unique individual taxpayer records. However, our review of the access logs did not identify unauthorized access to taxpayer records.

  The BEARS system sends notifications to the platform team when entitlements are changed or disabled. This notification prompts the platform team to take an action, such as removing the user. However, the platform team did not receive the notifications from BEARS for these [redacted] users when their entitlements were disabled. According to platform management officials, the BEARS entitlements were not set up correctly to send automatic notifications to the platform team. As a result, these users retained access to the platform. The platform team also identified the [redacted] users during their user account review and immediately took action to remove their access.

- **User accounts are not disabled as required.** We identified four user accounts that were not deactivated or disabled, as required. These users did not log into the platform for at least 90 calendar days but maintained their access to the system. Per the Internal Revenue Manual (IRM), after 90 days of inactivity, user accounts must be disabled. Since the IRS is not integrated with the Treasury Cloud, the platform management officials cannot disable inactive user accounts. Instead, they must rely on the Treasury Department to disable them, which occurs monthly. The process takes an additional two weeks for removal. The Treasury Department then provides the platform team a list of disabled users.

The platform contains more than 360 million unique individual taxpayer records and more than 160 million business taxpayer records. By not properly managing user access, the IRS cannot ensure that only users with appropriate business justifications have access to sensitive taxpayer data.

Recommendation 2: The Chief Information Officer should ensure that the responsible unit with the authority to remove Enterprise Data Platform user access is timely notified when appropriate *e.g.*, entitlements are changed or accounts are inactive.

> **Management's Response:** The IRS agreed with this recommendation and will ensure that the responsible unit with the authority to remove Enterprise Data Platform user access is timely notified in accordance with established policy.

The IRS still does not have a systemic process for recertifying user accounts

We found that the platform does not use systemic processes, *i.e.*, automated emails, alerts, *etc.*, to manage user access. The IRM states that automated mechanisms must be employed to support the management of system accounts. The process for automating the platform's account recertification was originally scheduled to be completed by the third quarter of FY 2025. However, according to platform management officials, the automation could not be achieved due to an infrastructure issue between IRS and Treasury networks. Specifically, the two networks do not have the appropriate trust relationship to allow secure, authenticated communication between them. The IRS estimates it will require an additional nine months to complete the automation process. In the meantime, the platform team has been manually reviewing user account access monthly.

Despite initially identifying the risk in January 2024, there is no active POA&M or Risk-Based Decision (RBD) to address the platform's lack of automated provisioning of user accounts. While the IRS does have a POA&M addressing the lack of Treasury integration, it does not directly relate to the platform's risk of manually reviewing user account access. In response to our findings, the platform management team created a draft RBD in July 2025 to address the identified risk. As of December 2025, the platform management team has not finalized the RBD addressing this issue.

Failing to automate the user account management process could lead to inefficiencies and improper access being granted. Additionally, failure to resolve or track existing weaknesses compromises the security posture of the platform, potentially exposing taxpayer data and information to unnecessary risk.

The Chief Information Officer should:

Recommendation 3: Coordinate with the Treasury Department to resolve the infrastructure issue between IRS and Treasury networks and ensure that systemic processes are incorporated into the platform user account management process once the infrastructure limitations are resolved.

> **Management's Response:** The IRS agreed with this recommendation and will coordinate with the Treasury Department to resolve the infrastructure issue between IRS and Treasury networks and ensure that systemic processes are incorporated into the

platform user account management process once the infrastructure limitations are resolved.

Recommendation 4: Establish a corrective action plan or an RBD to address the lack of automated provisioning of user accounts.

Management's Response: The IRS agreed with this recommendation and stated it has implemented corrective action. IRS Cybersecurity Memorandum, *Updated Authorization to Operate (ATO) Requirements for IRS Information Technology (IT) Systems*, dated November 14, 2025, directed the retirement of the RBD process in favor of leveraging the existing POA&M process. The Chief Information Officer has resolved this finding through POA&Ms. The associated risk is already actively tracked and managed through existing Enterprise Data Platform POA&Ms, and a new POA&M will be established to further strengthen coverage by explicitly addressing the risk associated with manual review of user access requests.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the Enterprise Data Platform data migration, capabilities, and security. To accomplish our objective, we:

- Assessed the progress of the data migration into the platform and its capabilities by reviewing the platform's data ingestion and capabilities roadmaps, verifying data ingestion and capabilities delivery efforts through documentation review, and interviewing management officials.
- Determined the effectiveness of platform's user access controls by reviewing IRM guidance and pertinent platform system security documents, analyzing user login activity reports, evaluating user accounts in the BEARS, reviewing the status of automation efforts and interviewing management officials.
- Determined whether the platform's user accounts are managed using the PUMAS by reviewing Federal and agency guidance related to privileged users, reviewing user accounts in the BEARS, and evaluating a list of platform's approved users.
- Determined the effectiveness and compliance of the process for documenting and remediating information security weaknesses within the platform by reviewing relevant National Institute of Standards and Technology and IRM guidance and evaluating whether Access Control POA&Ms are being created and reviewed timely.

Performance of This Review

This review was performed with information obtained from the Information Technology organization located at IRS headquarters in Washington, D.C. during the period October 2024 through December 2025. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

We performed tests to assess the reliability of data from the Enterprise Data Platform, the Assessment, Authorization and Risk Governance tool, the BEARS, the PUMAS, and the Strategic Implementation Management System. We evaluated the data by (1) interviewing agency officials knowledgeable about the data, (2) reviewing required data elements, (3) ensuring that the information was legible and contained alphanumeric characters, and (4) reviewing existing information about the data and the system that produced them. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for

planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Federal guidance from the National Institute of Standards and Technology and the IRM. We evaluated these controls by interviewing employees from the Information Technology organization and the Cybersecurity function, evaluating user account reports, assessing Access Control POA&Ms, and reviewing available documentation.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 2, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya,
Chief Information Officer
Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2026.05.02 14:27:24 -04'00'

SUBJECT: Draft Audit Report – The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform (Audit #2025208016)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. The IRS recognizes the need to address current gaps in entitlement management and will prioritize and resolve access control deficiencies with the Enterprise Data Platform.

Management agrees with the recommendations and have already begun taking corrective action. The IRS is committed to fully implementing and documenting all agreed-upon corrective actions. Please refer to the attachment for specific details.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 315-5000, or a member of your staff may contact Robert King, Coordinating Director, Data and Platform Engineering at (469) 801-1202.

Attachment

Attachment

Audit# 2025208016, *The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should work with the Treasury Department to ensure that privileged Enterprise Data Platform user accounts are fully integrated with the PUMAS.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will work with the Treasury Department to ensure that privileged Enterprise Data Platform user accounts are fully integrated with the PUMAS.

IMPLEMENTATION DATE: May 15, 2027

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should ensure that the responsible unit with the authority to remove Enterprise Data Platform user access is timely notified when appropriate *e.g.*, entitlements are changed, or accounts are inactive.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will ensure that the responsible unit with the authority to remove Enterprise Data Platform user access is timely notified in accordance with established policy.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Data and Platform Engineering

RECOMMENDATION 3: The Chief Information Officer should coordinate with the Treasury Department to resolve the infrastructure issue between IRS and Treasury networks and ensure that systemic processes are incorporated into the platform user account management process once the infrastructure limitations are resolved.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will coordinate with the Treasury Department to resolve the infrastructure issue between IRS and Treasury networks and ensure that systemic processes are incorporated into the platform user account management process once the infrastructure limitations are resolved.

IMPLEMENTATION DATE: February 15, 2027

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

Attachment

Audit# 2025208016, *The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform*

RECOMMENDATION 4: The Chief Information Officer should establish a corrective action plan or an RBD to address the lack of automated provisioning of user accounts.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation and has already implemented a corrective action. IRS Cybersecurity Memorandum, *Updated Authorization to Operate (ATO) Requirements for IRS Information Technology (IT) Systems*, dated November 14, 2025, directed the retirement of the RBD process in favor of leveraging the existing POA&M process. The Chief Information Officer has resolved this finding through POA&Ms. The associated risk is already actively tracked and managed through existing EDP POA&Ms, and a new POA&M will be established to further strengthen coverage by explicitly addressing the risk associated with manual review of user access requests.

IMPLEMENTATION DATE: June 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Data and Platform Engineering

Appendix III

Glossary of Terms

Term	Definition
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Business Entitlement Access Request System	A system that manages identity access management. It is used to request, modify, and remove access for active users to IRS systems by managing the digital identity of individuals, roles, resources, and entitlements granted or removed.
Dataset	A collection of data. This includes data procured from private third parties, data procured from other governments (foreign, Federal, State, local agencies), data collected for regulatory purposes, and data developed by combining data from multiple data sources.
Data Ingestion	The process of collecting, importing, transferring, or loading of raw data from diverse external sources into a centralized system or storage infrastructure, where it awaits further processing and analysis.
Entitlements	Access credentials that are granted based on the access patterns thereby allowing users to access specified data, tools, and environments on the platform.
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.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Plan of Action and Milestones	A corrective action plan to identify and document the resolution of information security weaknesses and periodically report to the Office of Management and Budget, the Treasury Department, and Congress.
Privileged Account	Accounts with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.
Privileged User	One that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Provisioning	A type of identity management responsible for creating, modifying or deleting user accounts and profiles. Access permissions and privileges are established and authentications are granted.
Risk-Based Decision	An approved decision for any accepted change to an operating system, database, web technology or application that causes that system to be out of compliance with the established security configuration.

Term	Definition
Secure Access Digital Identity Platform	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. Security Access Digital Identity is a major system that will deliver a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
Trust	A relationship established between domains that makes it possible for users in one domain to be authenticated by a domain controller in the other domain.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.
Universal Data Access	The ability to access and retrieve data from multiple, often diverse, data sources without being dependent on the underlying technology, format, or location of that data. It allows applications to connect to different types of databases and systems, such as relational, non-relational, or cloud-based data sources, providing a unified interface for data management. The concept of universal data access enables seamless data access and integration, making it easier for organizations to work with disparate data sources in a consistent and efficient manner.

Appendix IV

Abbreviations

BEARS	Business Entitlement Access Request System
FY	Fiscal Year
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones
PUMAS	Privileged User Management Access System
RBD	Risk-Based Decision
TIGTA	Treasury Inspector General for Tax Administration

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

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

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