

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



The IRS Needs To Improve Its Asset Retrieval Process for Departing Employees

August 24, 2026

Report Number: 2026-208-044

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

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

HIGHLIGHTS: The IRS Needs To Improve Its Asset Retrieval Process for Departing Employees

Final Audit Report issued on August 24, 2026

Report Number 2026-208-044

Why TIGTA Did This Audit

Since January 2025, the IRS has taken steps to reduce the size of its workforce. Approximately 22,000 employees departed the IRS from April through July 2025. These employees either voluntarily separated, accepted a Deferred Resignation Program offer, or took some other incentive to leave. The 22,000 employees were assigned more than 32,000 information technology assets. We evaluated the IRS's oversight and management of its information technology asset inventory for separated employees, including employees who participated in a Deferred Resignation Program.

Impact on Tax Administration

An information technology asset is property or equipment that is part of the information technology infrastructure. Information technology may include hardware and software assets. Hardware assets include laptops, network printers, smartphones, *etc.* Software assets include applications that allow IRS employees to access IRS systems using their personal devices through the IRS's Bring Your Own Device program.

Failing to collect assets from departing employees results in risk of data loss as well as a financial loss to the agency.

What TIGTA Found

We analyzed the records of 22,000 employees who departed from the IRS from April through July 2025. These employees were assigned more than 32,000 assets including laptops, portable printers, and smartphones. While most assets were returned, as of April 2026, the IRS still had not located 594 assets valued at more than \$270,000. However, IRS officials provided evidence that there were no instances of the employees accessing the IRS's network after their departure. In May 2026, Hardware Asset Management officials reached out to our Office of Investigations regarding these assets. We requested that the IRS provide additional documentation to support efforts to retrieve the missing assets before initiating an investigation, *i.e.*, evidence that the IRS tried to contact the employee to retrieve the missing assets.

While IRS policy requires assets to be returned upon departure, it does not include any specific time frame requirements. We found that this contributed to the inaccuracy of the asset inventory. Further, the IRS does not have a policy for recovering the costs of unreturned assets from departing employees. Therefore, there are no consequences if a departing employee fails to return their assets.

In addition, the IRS did not revoke access for a small number of personally owned device users. IRS policy requires that participants in the IRS's Bring Your Own Device program have their program access disabled upon departure. We analyzed the 52 Bring Your Own Device employees who separated from the agency and found 23 employees (44 percent) whose program access was not removed. However, IRS officials provided evidence that there were no instances of the employees accessing the network after their departure.

Finally, we found that audit trails for the asset management system were not being captured in the IRS's audit trail repository. IRS policy requires that system administrators enable, configure, and archive audit trails. However, the policy is not clear that audit trails must be added to the IRS's audit trail repository.

What TIGTA Recommended

We made four recommendations to improve the asset retrieval process, including updating policies to include specific time frames for returning assets, ensuring that necessary steps are taken to locate potentially stolen assets and that the necessary documentation to report the assets is provided to our Office of Investigations, adding audit trails to the audit trail repository for monitoring, and updating policies to clarify that system administrators must ensure that audit trails are sent to the repository, with instructions for how to do so.

The IRS agreed with our recommendations and plans to implement corrective actions.



**TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION**

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

August 24, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Needs To Improve Its Asset Retrieval
Process for Departing Employees (Audit No.: 2025208014)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) oversight and management of its information technology asset inventory for separated employees, including employees who participated in a Deferred Resignation Program. This review is part of our Fiscal Year 2026 Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

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

Table of Contents

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

Results of Review	Page 2
--------------------------------	--------

<u>IRS Policy Does Not Include Time Frames or Accurate Recordkeeping Controls To Account for the Information Technology Assets of Departing Employees</u>	Page 2
---	--------

<u>Recommendation 1:</u>	Page 3
--------------------------------	--------

<u>Recommendation 2:</u>	Page 4
--------------------------------	--------

<u>The IRS Did Not Revoke Access for a Small Number of Personally Owned Device Users</u>	Page 4
--	--------

<u>Audit Trail Data Are Not Captured in the Audit Trail Repository</u>	Page 4
--	--------

<u>Recommendations 3 and 4:</u>	Page 5
---------------------------------------	--------

Appendices

<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 6
--	--------

<u>Appendix II – Outcome Measure</u>	Page 8
--	--------

<u>Appendix III – Management’s Response to the Draft Report</u>	Page 9
---	--------

<u>Appendix IV – Glossary of Terms</u>	Page 13
--	---------

<u>Appendix V – Abbreviations</u>	Page 15
---	---------

Background

Since January 2025, the Internal Revenue Service (IRS) has taken steps to reduce the size of its workforce to comply with the President's executive orders and Office of Personnel Management guidance. Approximately 22,000 employees departed from the IRS from April through July 2025. These employees either voluntarily separated, accepted a Deferred Resignation Program (DRP) offer, or took some other incentive to leave.¹ IRS policy requires that the information technology assets, *i.e.*, hardware or software, of employees be returned and that their access to software applications be disabled upon their departure.

Information technology assets

The IRS's Information Technology (IT) organization is responsible for asset management policies. Information technology may include hardware and software assets.

Hardware assets

Hardware assets include laptops, portable printers, smartphones, *etc.* The IRS maintains its hardware asset inventory using the Internal Revenue Workflow Optimization, Request and Knowledge System - Hardware Asset Management application (hereafter referred to as the asset management system).

The IRS follows its Separating Employee Clearance (SEC) process to retrieve the assets of separating employees.² The IRS generally followed this same process for employees who departed as part of a DRP.³ The SEC process consists of:

- 1. Submitting a Personnel Action Request** – The process is initiated when either the employee, manager, or human resource specialist submits a personnel action request.
- 2. Creating an SEC Record** – Upon approval of the personnel action request, an SEC record is created in the IRS's human resources system. In addition, a service ticket is created within the asset management system.
- 3. Obtaining a List of Assets** – Managers enter the separating employees' unique Standard Employee Identifier into the asset management system. Managers must also manually update the SEC record in the human resources system with the asset information.
- 4. Retrieving Assets** – Local IT employees are notified by the asset management system that assets need to be retrieved from local separating employees. These IT employees retrieve the assigned assets from the employee and/or their manager and send the assets to the IT depot. The IT depot is a centralized storage area for in-stock IT equipment.

¹ See Appendix III for a glossary of terms.

² *Hardware Asset Management User Guide* (Sept. 2019).

³ The DRPs allowed federal employees to resign with pay through September 30, 2025, or later, if the employee's retirement date was between October 1 and December 31, 2025. The IRS altered the SEC process for the DRPs to systemically create tickets within the asset management system, bypassing step one, and part of step two.

5. **Updating the Asset Management System** – Local IT employees update the system once they retrieve assets. Similarly, an employee at the IT depot will update the system once they receive the asset.
6. **Reporting Unrecovered Assets** – If an asset is not retrieved, the manager is required to report this to the IRS's Computer Security Incident Response Center (CSIRC). CSIRC reports stolen assets to our Office of Investigations. Missing assets are updated within an internal tracking system. If an asset is later located, CSIRC will update the internal tracking system. The asset management system will also be updated. However, CSIRC does not attempt to locate the missing assets.
7. **Release of SEC Record** – Employees in the IRS's asset management group confirm the accuracy of the asset inventory by reviewing the ticket against the SEC record. If there are discrepancies, they work with the employee's manager to resolve them. Once confirmed, the asset management group clears the SEC record.

Software assets

Software assets include applications that allow IRS employees to access IRS systems using their personal devices. This is accomplished through the IRS's Bring Your Own Device (BYOD) program. The IRS maintains user's access to software assets using the Business Entitlement Access Request System (BEARS).

When an individual's employment status changes, a personnel action request is generated and transmitted automatically to the BEARS. The BEARS then automatically notifies the applications the user had access to. The process to remove the user's access is specific to each application. Some applications systemically remove access, while some applications require manual removal of the user's access. We have a separate review ensuring that system access was removed for DRP participants.

Results of Review

IRS Policy Does Not Include Time Frames or Accurate Recordkeeping Controls To Account for the Information Technology Assets of Departing Employees

We analyzed the records of approximately 22,000 employees who departed from the IRS from April through July 2025. These employees were assigned more than 32,000 assets. Although most assets were returned, our analysis identified 1,308 assets (4 percent) that showed as not returned as of November 2025. We shared the listing of these assets with IRS IT. We recommended that IT perform a reconciliation to locate these assets and update the asset management system. As of April 2026, the IRS has still not located 594 assets valued at more than \$270,000. These assets included laptops and smartphones.

While IRS policy requires assets to be returned upon departure, it does not include any specific time frame requirements. We found the lack of guidance contributed to the inaccuracy of the asset inventory as of November 2025. In addition, the lack of reconciliation processes to ensure that assets were returned by departing employees also impacted the accuracy of the inventory. For example, we found that:

- Managers who collected the assets from their onsite employees did not return the assets. The assets should have been returned to the local IT office, but many were not until the IRS completed the reconciliation of the 1,308 assets.
- Local IT offices did not ship assets to the IT depots and/or update the asset management system upon receipt.
- IT depot employees were not updating the status of returned assets in the asset management system upon receipt.

Further, the IRS does not have a policy for recovering the costs of unreturned assets from departing employees. Therefore, there are no consequences if a departing employee does not return their assets. Failing to collect assets from departing employees results in a financial loss to the agency. In addition, the IRS is unable to reuse the assets, potentially causing the agency to purchase new assets for other employees.

The IRS attempted to locate these assets for months by contacting the employee's manager, checking local IT offices, and checking IT depots. Hardware Asset Management officials stated that 714 assets were located as of April 2026. However, 594 assets were not. Further, Hardware Asset Management officials provided evidence that there were no instances of the employees accessing the IRS's network after their departure.

In May 2026, the asset management system was updated, and the 594 assets were reported to CSIRC as lost. Hardware Asset Management officials also contacted our Office of Investigations to report the assets as stolen. Our Office of Investigations requested additional documentation from the IRS, *i.e.*, evidence that management tried to contact the employee to retrieve the missing assets, before initiating an investigation. To date, Hardware Asset Management officials have not taken additional steps to locate the missing assets.

As previously noted, CSIRC does not attempt to locate missing assets. CSIRC only reports stolen assets to our Office of Investigations. As these employees have separated from the IRS, we believe these assets should be considered stolen as opposed to missing. The IRS cannot locate the items, and they have no evidence that the assets were returned by the employees. These assets place the IRS at risk of data loss as the hard drives of laptops and memories of smartphones have not been cleared and could contain sensitive taxpayer information.

The Chief Information Officer should:

Recommendation 1: Update its policy to include specific time frames for returning assets of departing employees and updating inventory records. In addition, establish processes to ensure that these policies are followed.

Management's Response: IRS management agreed with this recommendation and will update applicable policies to establish time frames for returning assets and updating inventory records and will implement monitoring processes to ensure compliance.

Recommendation 2: Ensure that the necessary steps are taken to locate potentially stolen assets and prepare the necessary documentation to report the assets to TIGTA's Office of Investigations.

Management's Response: IRS management agreed with this recommendation and will strengthen procedures to ensure that reasonable efforts are taken to locate potentially lost or stolen assets and that appropriate documentation is prepared to support timely referral to TIGTA's Office of Investigations, as appropriate.

The IRS Did Not Revoke Access for a Small Number of Personally Owned Device Users

IRS policy requires that participants in the IRS's BYOD program have their program access disabled upon departure. However, our analysis of the 52 BYOD employees who separated from the agency from February through July 2025 found:

- 23 employees (44 percent) whose program access was not removed.
- 29 employees (56 percent) whose program access was removed.

The 23 employees who were not removed from the BYOD program were part of a DRP. For employees who departed via a DRP, the IRS did not follow established procedures for revoking BYOD program access. Instead, the IRS's Human Capital Office provided IT with a list of departing DRP employees and IT personnel decided only to remove employees that had an assigned administrative leave date. This decision was based on the uncertainty regarding whether the employees had rescinded their acceptance into a DRP.

On October 1, 2025, we alerted the IRS of our concern and recommended that the 23 employees have their access to the BYOD program immediately removed.

Management Action: End User Digital Services management officials agreed and removed the 23 employees' BYOD access as of October 2, 2025. Officials also provided evidence that there were no instances of the 23 employees accessing the IRS's network after their departure.

Audit Trail Data Are Not Captured in the Audit Trail Repository

The IRS's asset management system was placed into production on a cloud-based platform in November 2024. This means that the data within the asset management system is stored on remote servers managed by a third-party. However, the required audit trail data for this system are not captured in the IRS's audit trail repository. Audit trail data are important so that Cybersecurity can monitor a system for inappropriate use. According to staff from the IRS's audit trail repository team, they were not aware that this cloud-based asset management system existed and that audit trails needed to be added to the repository.

IRS policy requires that system administrators enable, configure, and archive audit trails. However, the IRS's policy does not provide clear guidance regarding how audit trail data are to be transmitted to the repository. The administrator responsible for the asset management system acknowledged the policy but felt they were meeting the requirements since the cloud-based platform was configured to track auditable events. They were unaware that the audit trail data should have also been transmitted to the repository.

Without the availability of required audit trail data, Cybersecurity is unable to [REDACTED]
[REDACTED] This increases the risk that [REDACTED]. In

August 2025, we alerted IT management of our concern. Management officials from IT's Infrastructure Technical Operations agreed with our concern and developed a plan to accomplish the desired outcome.

The Chief Information Officer should ensure that:

Recommendation 3: Audit trails for the cloud-based asset management system are added to the IRS's audit trail repository and monitored as planned.

Management's Response: IRS management agreed with this recommendation and will complete integration of audit trail data for the cloud-based asset management system into the centralized audit trail repository and begin monitoring those audit trails.

Recommendation 4: Relevant IRS policies are updated to clarify that system administrators, including cloud-based systems, must send audit trails to the IRS's repository and include instructions for how to do so.

Management's Response: IRS management agreed with this recommendation and will validate that existing policy governing audit trail requirements for system administrators, including cloud-based systems, is current and clear. The Chief Information Officer will also ensure that the Internal Revenue Manual provides a working link to the Enterprise Security Audit Trails Standard Operating Procedures, which include instructions for forwarding audit logs to a centralized repository.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's oversight and management of its information technology asset inventory for separated employees, including employees who participated in a DRP. To accomplish our objective, we:

- Determined if all hardware assets were retrieved from departing employees. We obtained an extract of all assessment management data as of April 2025, and again as of November 2025. IRS reports associated with asset management were unavailable before April 2025. Therefore, we were only able to determine whether assets were returned for employees who departed from April through July 2025.
- Determined if all devices from the IRS's BYOD program were disabled for departing employees from February through July 2025.
- Determined whether the IRS enabled, configured, reviewed, and archived audit trails for the asset management system.

Performance of This Review

This review was performed at the IRS IT depot in Memphis, Tennessee, and local IRS IT offices in Oakland, California; Kansas City, Missouri; and Houston, Texas along with information obtained from the IRS's Cybersecurity and End User Digital Services functions located in Lanham, Maryland, and from the Infrastructure Technology Operations function located in Philadelphia, Pennsylvania during the period April 2025 through March 2026. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

We performed tests to assess the reliability of data that we pulled from the following sources:

- The Treasury Integrated Management Information System as of July 2025.
- The Single Entry Time Reporting System as of July 2025.

We evaluated the data by: (1) performing electronic testing of required data elements, and/or (2) reviewing existing information about the data and the system that produced them. We determined that the data were sufficiently reliable for purposes of this report.

We also performed applicable tests to assess the accuracy and completeness of the following data that was provided by the IRS:

- Asset management system data as of April 2025 and November 2025.
- BEARS data for active and inactive BYOD users as of August 2025.

- BEARS data for active and inactive local area network entitlement users as of October 2025.
- Mobile access solution data as of August 2025.

We determined that the data were sufficiently reliable for 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: the process for retrieving departing employees' assets, updating asset management system, and disabling BYOD devices. We evaluated these controls by reviewing IRS's policies and procedures, meeting with IRS subject matter experts responsible for the process and conducting site visits to physically view the process.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

- Funds Put to Better Use – Potential; \$274,822 for the 594 assets that were not returned from IRS employees who separated from April through July 2025 (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We identified 12,602 IRS employees who had separated from the IRS from February through July 2025, from the Treasury Integrated Management Information System data extract. We also identified 22,196 IRS employees who reported a DRP code in the Single Entry Time Reporting System from February through July 2025. Of the 34,798 employees identified (12,602 + 22,196), we determined that there were 31,035 unique employees. An employee who was part of a DRP could have resigned from their position and thus also separated from the IRS.

Of the 31,035 unique employees, we determined 22,487 employees separated or accepted a DRP after April 2025. This date was used to coincide with the date of our first asset management data extract. We matched the 22,487 unique employees to the asset management data extract as of April 2025 and identified more than 32,000 assets associated with those employees. We then matched the unique asset numbers to the November 2025 asset management extract to determine the status of the assets. Based upon the status field, we identified 1,308 assets that did not show as returned as of November 2025. The IRS completed a reconciliation and located some of these assets. However, as of April 2026, the IRS still could not locate 594 assets valued at \$274,822. This cost is what was reflected in the IRS's asset management system.

Appendix III

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 30, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya,
Chief Information Officer

Donald C. Drake
Digitally signed by Donald C. Drake
Date: 2026.07.30 15:14:23 -04'00'

SUBJECT: Draft Audit Report – The IRS Needs to Improve its Asset Retrieval Process for Departing Employees (Audit #2025208014)

The Internal Revenue Service (IRS) appreciates the opportunity to review and respond to the draft audit report. The IRS recognizes the importance of maintaining effective controls over information technology assets and remains committed to strengthening processes that protect taxpayer information while ensuring accountability for government property.

Management concurs with all four recommendations. The IRS will update applicable policies, strengthen asset retrieval and recovery processes, complete audit trail integration and monitoring for the cloud-based Hardware Asset Management system, and validate that applicable policy contains audit trail requirements for system administrators, including cloud-based systems, and provides a reference to the process for forwarding audit logs to the centralized repository. While the IRS can establish and communicate policy requirements, its ability to compel compliance is limited when individuals do not comply with those requirements. For cases in which individuals refuse to return the IRS-issued equipment, the IRS will request assistance from the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations, as appropriate, to support asset retrieval efforts and any necessary investigative follow-up. Please refer to the attachment for specific details.

The IRS also acknowledges TIGTA's reported outcome measure of \$274,822. Following TIGTA's review, the IRS continued reconciliation efforts, resulting in additional assets being located and inventory records being updated. As reconciliation efforts continue, the final financial impact may differ from the amount reported in the draft audit report.

2

The IRS appreciates the continued oversight and review provided by your office. If you have any questions, please contact me or a member of your staff may contact Tanya Chiaravalle, Coordinating Director, End User Digital Services, at (240) 613-4255.

Attachment

Attachment

**Internal Revenue Service (IRS) Management Response to Treasury Inspector General for
Tax Administration's (TIGTA) Draft Report**
The IRS Needs to Improve its Asset Retrieval Process for Departing Employees
Audit #2025208014

Recommendations

RECOMMENDATION 1: The Chief Information Officer should update its policy to include specific time frames for returning assets of departing employees and updating inventory records. In addition, establish processes to ensure that these policies are followed.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will update applicable policies to establish time frames for returning assets and updating inventory records and will implement monitoring processes to ensure compliance.

IMPLEMENTATION DATE: December 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

RECOMMENDATION 2: The Chief Information Officer should ensure that the necessary steps are taken to locate potentially stolen assets and prepare the necessary documentation to report the assets to TIGTA's Office of Investigations.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will strengthen procedures to ensure reasonable efforts are taken to locate potentially lost or stolen assets and that appropriate documentation is prepared to support timely referral to TIGTA's Office of Investigations, as appropriate.

IMPLEMENTATION DATE: December 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

RECOMMENDATION 3: The Chief Information Officer should ensure that audit trails for the cloud-based asset management system are added to the IRS's audit trail repository and monitored, by August 2026, as planned.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will complete integration of audit trail data for the cloud-based asset management system into the centralized audit trail repository and begin monitoring those audit trails.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure Tech Ops

RECOMMENDATION 4: The Chief Information Officer should ensure that relevant IRS policies are updated to clarify that system administrators, including cloud-based systems, must send audit trails to the IRS's repository and include instructions for how to do so.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will validate that existing policy governing audit trail requirements for system administrators, including cloud-based systems, is current and clear. The Chief Information Officer will also ensure the Internal Revenue Manual provides a working link to the Enterprise Security Audit Trails Standard Operating Procedures, which include instructions for forwarding audit logs to a centralized repository.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Bring Your Own Device	An IRS program that allows IRS employees to use their personally owned technology devices to stay connected to, access data from, or complete tasks for their organizations.
Business Entitlement Access Request System	An IRS service-wide system used to register users for access to any IRS information technology resource that they require access.
Cloud-Based	A computing model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources, <i>e.g.</i> , network, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction.
Computer Security Incident Response Center	An IRS team of capable “first responders” who are organized, trained, and equipped to identify and eradicate cyber threats or cyberattacks. One of its primary duties is to provide 24-hour monitoring and support for IRS operations seven days a week, 365 days a year.
Deferred Resignation Programs	Programs that allowed employees to resign from their positions as of September 30, 2025, or December 31, 2025, while remaining on paid administrative leave until that time.
End User Digital Services	Delivers secure, modern, and responsive technology services that enable IRS employees to work efficiently, collaborate effectively, and support taxpayers from any location.
IT Depot	A centralized storage area where the IRS stores stock assets.
Infrastructure Technical Operations	Provides secure, scalable, and high-performance IT infrastructure and user support services that form the operational foundation for IRS systems.
Internal Revenue Workflow Optimization, Request and Knowledge System - Hardware Asset Management	The authoritative source for all hardware asset management and inventory information within the IRS and supersedes other inventory data sources. It is the official IRS centralized asset management inventory database of all IT and non-IT personal property that meets the specified threshold/reportable criteria. It is a subsidiary account to the general ledger for managing personal property and tracks each item of accountable property through the asset’s lifecycle (acquisition through final disposal).
Local Area Network	A group of computers and associated devices that share a common communications line or wireless link to a server. Typically encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment. Computers and other mobile devices use the connection to share resources such as a printer or network storage.

Term	Definition
Single Entry Time Reporting System	An online payroll system in the Totally Automated Personnel System that enables the input of Time and Attendance data to the National Finance Center.
Standard Employee Identifier	A five-digit code that uniquely ties employees to their data without using their Social Security Number.
Treasury Integrated Management Information System	An official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. It is outsourced to the U.S. Department of Agriculture's National Finance Center and managed by the Department of the Treasury.

Appendix V

Abbreviations

BEARS	Business Entitlement Access Request System
BYOD	Bring Your Own Device
CSIRC	Computer Security Incident Response Center
DRP	Deferred Resignation Program
IRS	Internal Revenue Service
IT	Information Technology
SEC	Separating Employee Clearance
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.