TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Systems Hosting Sensitive Data Lack Consistent Inventory Standards

March 26, 2025

Report Number: 2025-200-009

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

HIGHLIGHTS: Systems Hosting Sensitive Data Lack Consistent Inventory Standards

Final Audit Report issued on March 26, 2025 **Report Number 2025-200-009**

Why TIGTA Did This Audit

In September 2020, the National Institute of Standards and Technology published guidance requiring organizations to develop an inventory of system components that accurately reflects the system and is appropriate for tracking and reporting. The IRS has five different data sources for tracking the inventory of its systems, four of which we were able to use in this audit.

This audit was initiated to determine whether the IRS has an effective process to consistently identify systems and applications and track sensitive data held on these systems across multiple inventory systems.

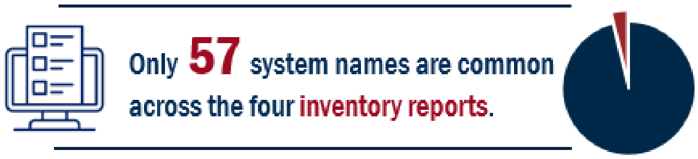
Impact on Tax Administration

A consistent classification of IRS systems is required to ensure that all systems with access to sensitive data are identified and taxpayer data are safeguarded. An important first step is ensuring that all systems are identified and maintained in an authoritative inventory. Improper inventory management could compromise the IRS's ability to ensure appropriate access controls.

In addition, unreliable information in the user access request system, which reports Personally Identifiable Information (PII) and Federal Tax Information (FTI) designations in IRS systems, will result in inaccurate reporting whether authorized users are granted the appropriate access to IRS systems.

What TIGTA Found

The IRS does not have an effective systems inventory management process. For example, the process for implementing new systems does not include a step to notify the authoritative inventory owner. We analyzed data from four inventory data sources and generated a list of 1,410 unique IRS system names.



Only **57** system names are common across the four inventory reports.

We focused our detailed analysis on the 176 systems in the master inventory owned and maintained by the Cybersecurity function. We determined that:

- 82 systems (47 percent) were included in all inventory reports but were inconsistently named.
- 57 system names (32 percent) matched across all 4 inventory reports.
- 26 systems (15 percent) had a valid reason for not being included in all four inventory reports.
- 11 (6 percent) systems were missing from one or more of the required inventory systems.

Three of the four inventory reports we analyzed record whether an IRS system contains PII and FTI. We identified inconsistencies between the inventory reports with respect to whether a particular system contained PII or FTI. We compared all 59 systems that were consistently named across the 3 inventory reports. We determined that 52 (88 percent) were consistently identified as containing PII and FTI and 7 systems (12 percent) were not.

The IRS updated guidance that should ensure that new systems are added to the authoritative inventory system as the first step in the deployment process, with a system name that meets standards, and which will be used in all other IRS inventory systems.

What TIGTA Recommended

We recommended that the Chief Information Officer should:
1) require approval that new system names meet naming standards;
2) require a unique identifier in the authoritative inventory be implemented and applied to the other inventory systems; 3) conduct an annual reconciliation of the multiple inventory systems; and
4) improve its annual validation process to ensure that all systems with PII and FTI are consistently designated across the multiple inventory systems.

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

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

March 26, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Danny Verneuille

FROM: Danny Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Systems Hosting Sensitive Data Lack Consistent Inventory Standards (Audit No.: 2024200023)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has an effective process to consistently identify systems and applications and track sensitive data held on these systems across multiple inventory systems. This review was part of our Fiscal Year 2024 Annual Audit Plan 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. If you have any questions, please contact me or Linna Hung, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

In September 2020, the National Institute of Standards and Technology published guidance requiring organizations to develop an inventory of system components that accurately reflects the system and is appropriate for tracking and reporting.[1] Organizations may choose to implement centralized system component inventories that include components from all organizational systems. According to the Information Technology organization's Cybersecurity function, the Internal Revenue Service (IRS) has five different data sources for tracking the inventory of its systems:

1. The As-Built Architecture (ABA) – the authoritative source for business systems in production. The ABA is owned and maintained by the Information Technology organization's Enterprise Services function.
2. The Federal Information Security Modernization Act of 2014 (FISMA) Master Inventory – according to the IRS, it is a record of the IRS's uniquely FISMA reportable boundaries that includes general support systems, major systems, and minor systems.[2] It also reflects other systems and/or components as part of the uniquely reportable general support system, major system, and minor system boundaries as defined by FISMA guidelines. The number of reportable boundaries in the FISMA Master Inventory is significantly lower than other inventory systems because many systems are comprised of multiple systems/components that make up that uniquely reportable boundary whereas these systems/components are listed individually in other inventory systems. The FISMA Master Inventory is owned and maintained by the Cybersecurity function.
3. The Privacy Impact Assessment Management System (PIAMS) – the official repository for systems requiring a Privacy and Civil Liberties Impact Assessment. The PIAMS is owned and maintained by the Privacy, Governmental Liaison and Disclosure Office.
4. The Enterprise Security Audit Trails (ESAT) Tracker – a combination of the ABA, the FISMA Master Inventory, and the PIAMS. The ESAT Tracker is owned and maintained by the Cybersecurity function.
5. The Treasury FISMA Inventory Management System – the official repository of information systems reported under FISMA. This system is owned and maintained by the Department of the Treasury, so we did not analyze its data.

Results of Review

We met with IRS management officials responsible for each of the inventory systems to discuss the processes for naming, adding, and managing an IRS system. Each group has its own standard operating procedures for inventory management. As a result, there is not a standardized process for entering IRS systems into all inventory systems. This is significant

[1] National Institute of Standards and Technology, Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5 (September 2020). See Appendix IV for a glossary of terms.

[2] 44 U.S.C. §§ 3551-3558 (2018).

because most of the IRS's systems contain sensitive data, such as Personally Identifiable Information (PII) and Federal Tax Information (FTI). Without consistent classification, the IRS cannot ensure that sensitive data is correctly identified and protected. In addition, improper inventory management could compromise the IRS's ability to ensure appropriate access controls.

The IRS's Systems Inventory Management Process Is Not Effective

We obtained the inventory reports from the ABA, the FISMA Master Inventory, the PIAMS, and the ESAT Tracker from November through December 2023, totaling 2,306 systems identified between the 4 inventory systems. Figure 1 illustrates the number of IRS systems from each inventory report.

Figure 1: IRS System Inventory Reports

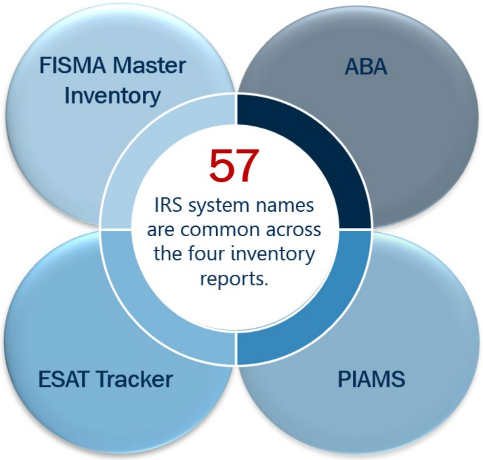
Inventory Report Source	Number of Systems
ABA	731
FISMA Master Inventory	176
PIAMS	526
ESAT Tracker	873
Total of Systems	**2,306**

Source: Analysis of IRS inventory reports.

From this population, we eliminated duplicates, which generated a list of 1,410 unique systems.[3] We then evaluated the effectiveness of the IRS's process to identify and track IRS systems across its multiple inventory systems. We focused our detailed analysis on the 176 systems in the FISMA Master Inventory owned and maintained by the Cybersecurity function. From the 4 inventory reports, we identified 57 systems that consistently used the same IRS system name across all the inventory reports. Figure 2 illustrates our results.

[3] Systems could be listed in multiple inventory reports.

Figure 2: System Inventory Report Comparison


FISMA Master Inventory
ABA
57
IRS system names are common across the four inventory reports.
ESAT Tracker
PIAMS

Source: Analysis of IRS inventory reports.

However, we identified three issues: 1) the system development process did not include a formal engagement with the authoritative inventory system owner; 2) many IRS systems were named inconsistently across the inventory reports; and 3) some IRS systems that met requirements to be included in an inventory system were not appropriately added.

The authoritative inventory system owner was not formally engaged

The IRS uses a One Solution Delivery Life Cycle (OneSDLC) process (*i.e.*, the compliance process) for implementing new IRS systems. However, the process did not include a step for adding new IRS systems to its authoritative inventory system, the ABA. According to Enterprise Services function management, it relies on customers and/or other functions, such as the Applications Development function, the Enterprise Operations function, or the Cybersecurity function, to notify them of new IRS applications and systems. Even when Enterprise Services function personnel are aware of new IRS systems, they are not added to the ABA early in the development process.

According to the IRS, the OneSDLC process facilitates transparency and collaboration, in support of early and often product delivery. The purpose of the process is to help system owners complete all requirements prior to deployment and to avoid delays caused by not engaging with the appropriate process owners. Enterprise Services function management stated that engaging the ABA team and obtaining its approval is not a required step in the OneSDLC Compliance List. This increases the risk that the IRS may have systems in production that are not part of its authoritative inventory system.

In June 2024, the IRS updated its OneSDLC Compliance List to include a new first step in the deployment process to engage the ABA team via email, prior to the creation of the project charter. The purpose of this new step is to establish a system name that meets ABA naming standards and formally creates Ian authoritative record in the ABA, including the unique ABA Number. The ABA approved system name and unique ABA Number will be applied to all project artifacts and should flow to the other IRS inventory systems. We verified that the OneSDLC guidance was updated with a new step to engage the ABA team. However, the IRS did not create an approval step as part of its update.

Recommendation 1: The Chief Information Officer should require that ABA team approval be obtained to ensure that new system names meet naming standards and authoritative records are formally created in the ABA and used throughout the other IRS inventory systems.

> **Management's Response:** The IRS agreed with this recommendation and will implement a naming standard process requiring adequate approval.

IRS systems were not consistently identified

Due to the large number of inconsistencies between inventory numbers and IRS system names, we focused on attempting to reconcile the three other inventory systems to the FISMA Master Inventory. We compared 176 systems in the FISMA Master Inventory (as of December 2023) with those found in the ABA, the PIAMS, and the ESAT Tracker inventory reports. Figure 3 illustrates our findings.

Figure 3: FISMA Master Inventory Reconciliation to the Three Other IRS System Inventory Reports

	Number of Systems With Mismatched Names Across Inventory Reports	Number of Systems Not in an Inventory Report With a Valid Reason	Number of Systems Not in an Inventory Report Without a Valid Reason	Total Number of Systems
Match Across All Three Other Inventory Reports	N/A	N/A	N/A	57
Match Across Two Other Inventory Reports	12	3	0	15
Match Across One Other Inventory Report	23	11	5	39
System Only in the FISMA Master Inventory	47	12	6	65
Total Systems				**176**

Source: Analysis of the IRS's inventory reports.

Specifically, we identified that the names of 57 (32 percent) of the 176 IRS systems in the FISMA Master Inventory matched across the other 3 inventory reports. Of the 176 IRS systems, we also identified:

- 82 (47 percent) IRS systems were included in all inventory reports but were inconsistently named. Most of the system naming discrepancies were a result of a lack of standardization. A lack of consistent and accurate system names impacts the IRS's ability to identify and reconcile systems and protect taxpayer data. Examples of inconsistencies identified include:
  - System names that did not match because they were entered into one or more inventory systems with the system name spelled out versus using an acronym in the name (*e.g.*, Affordable Care Act versus ACA).

- System names that did not match because of the inclusion of special characters like “&” in place of "and” or using a “- “in some entries but not others.
- System names that did not match because a word in the name was entered as singular instead of plural (*e.g.*, Account versus Accounts).

- 26 (15 percent) IRS systems were not added to the other inventory systems. However, acceptable justifications were available for their omission. For example, IRS systems that did not require a Privacy and Civil Liberties Impact Assessment would not need to be in the PIAMS.
- 11 (6 percent) IRS systems were missing from one or more required inventory systems. We found that these systems were not added but met the requirements to be in one of the other three inventory systems and did not have a valid reason for its omission

According to the Internal Revenue Manual, an inventory of systems shall be developed and updated as systems are commissioned and decommissioned, and at a minimum, annually. In addition, the National Institute of Standards and Technology requires that the IRS develop and document an inventory of system components that accurately reflects the system; includes all components of a system; and does not include duplicate accounting of components or components assigned to any other system. It also states that using a consistent system name is necessary for effective and efficient accountability of system components.

In addition, the IRS does not have a standardized process (*e.g.*, a unique system identifier) for entering IRS systems into all its inventory systems and lacks a comprehensive reconciliation process to ensure that its multiple inventory systems are consistent with each other. As a result, IRS systems are often entered into inventory systems differently and there is no unique identifier to associate the IRS system between inventory systems.

The IRS created an ABA Number to uniquely identify each system. However, the ESAT Tracker is the only inventory system that incorporates the ABA Number. The lack of a unique system identifier in each inventory system significantly complicates and may hinder the reconciliation process, resulting in the Cybersecurity function conducting significant research across multiple functional areas to validate the disparate inventories.

A consistent classification is required to ensure that all IRS systems with access to sensitive data are identified and taxpayer data are safeguarded. An important first step is ensuring that all IRS systems are identified and maintained in an authoritative inventory. Without a consistent and accurate inventory of systems, there is an increased risk that the IRS would be unable to maintain internal controls. In addition, there is an increased risk that taxpayer data in these IRS systems would not be adequately protected if the system is not correctly added to necessary inventory systems.

The lack of a consistent classification of IRS systems and the unreliability of the data prevented us from completing one specific test. We attempted to match the IRS system name from the user access system report with the other inventory reports to perform a comparison of PII and FTI designations. However, we found that over 90 percent of the IRS system names did not match between the user access request system and the multiple inventory systems. Cybersecurity function management confirmed that PII and FTI designations in the user access request system are not reliable. Unreliable information in the user access request system, which reports PII and FTI designations in IRS systems, will result in inaccurate reporting whether authorized users are granted access to IRS systems containing PII and FTI. We reported similar issues obtaining a complete and reliable inventory of sensitive systems in February 2024.[4]

The Chief Information Officer should:

Recommendation 2: Require a unique system identifier for each new and legacy system in the authoritative inventory be implemented and applied to system records in the other inventory systems.

> **Management's Response:** The IRS agreed with this recommendation and stated that a unique identifier has been established within the authoritative inventory and will be used to align and update system records across the other inventory systems.

Recommendation 3: Conduct an annual reconciliation of the multiple inventory systems to ensure that all systems are using unique system identifiers.

> **Management's Response:** The IRS agreed with this recommendation and will perform a yearly reconciliation of the multiple inventory systems to verify that each system is assigned and using a unique system identifier.

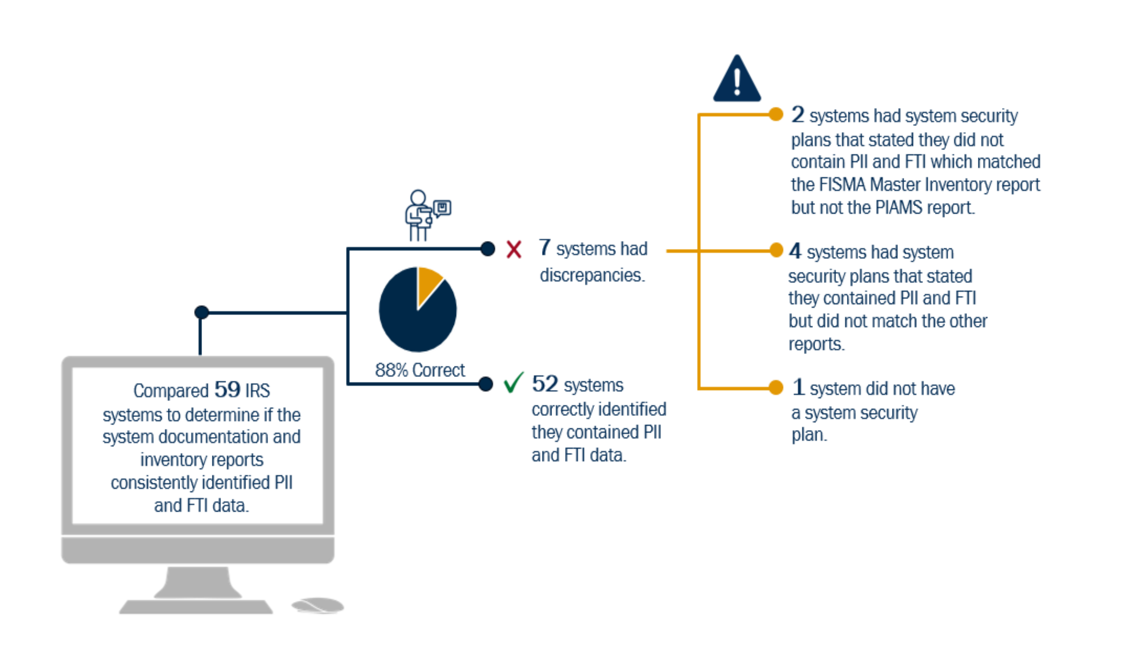
IRS Systems Containing Sensitive Data Were Not Consistently Tracked Across Inventory Systems

Several IRS systems contain sensitive information. We selected all 59 IRS systems that were consistently named between the 3 inventory reports that track PII and FTI: the PIAMS, the FISMA Master Inventory, and the ESAT Tracker. We compared the inventory reports, along with the IRS system security plans, to identify how many inventory reports were consistently tracking IRS systems containing sensitive data.[5] Figure 4 illustrates the number of systems with PII and FTI designation discrepancies.

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

[5] The audit team did not review data on any system to conclude that systems with PII and FTI were inconsistently tracked between different inventories and/or the system security plans.

Figure 4: PII and FTI Designations Were Inconsistent


Compared 59 IRS systems to determine if the system documentation and inventory reports consistently identified PII and FTI data.
88% Correct
✗ 7 systems had discrepancies.
✓ 52 systems correctly identified they contained PII and FTI data.
2 systems had system security plans that stated they did not contain PII and FTI which matched the FISMA Master Inventory report but not the PIAMS report.
4 systems had system security plans that stated they contained PII and FTI but did not match the other reports.
1 system did not have a system security plan.

Source: Analysis of the IRS's inventory reports.

- 52 (88 percent) consistently identified the systems as containing PII and FTI across the 3 inventory reports.
- 7 (12 percent) had discrepancies across the 3 inventory reports as to whether the system contained PII and FTI. The FISMA Master Inventory PII and FTI designation did not match the PIAMS inventory report on any of the seven systems. We conducted additional analysis of the 2023 system security plans for the seven systems and found that:
  - 4 IRS systems had system security plans that stated the system did contain PII and FTI but did not match the PIAMS report nor the FISMA Master Inventory report. In addition, we reviewed the prior year system security plans and found that all four of these systems were designated as having PII and FTI.
  - 2 IRS systems had system security plans that stated the system did not contain PII and FTI which matched the FISMA Master Inventory report but did not match the PIAMS report.
  - 1 IRS system did not have a system security plan for us to determine whether it should or should not be designated as having PII or FTI data but was inconsistently reported between the 3 inventory reports.

The Office of Management and Budget requires agencies to maintain an inventory of its information systems that collects, processes, stores, maintains, disseminates, or discloses PII (which includes FTI) to allow the agency to regularly review the PII and ensure that it is accurate, relevant, timely, and complete.[6] Further, according to an August 2023 Government

[6] Office of Management and Budget, Circular A-130 Revised, Managing Information as a Strategic Resource (July 2016).

Accountability Office report, ensuring that system information is accurate will help the IRS maintain a comprehensive inventory of systems that process or store taxpayer information.

According to Cybersecurity function management, they review systems security plans to obtain information regarding the PII and FTI designation. Management officials also stated that they have not received a FISMA Change Request from the application owner for any of the seven systems that contain PII and/or FTI. In addition, they conduct an annual validation of all data fields in the FISMA Master Inventory report with key system points of contact. However, we identified four systems where both the FISMA Master Inventory PII and FTI designation were incorrect, and the errors were not identified during the annual validation. By not maintaining a comprehensive inventory system, the IRS cannot ensure that it has implemented safeguards to protect taxpayer information being processed or stored on all of its systems, applications, and databases. Further, having a comprehensive inventory would enable the IRS to monitor all relevant systems that process taxpayer information to detect when its staff accesses taxpayer information without authorization.

Recommendation 4: The Chief Information Officer should improve its annual validation process to ensure that all systems with PII and FTI inventory data are consistently designated across the multiple inventory systems, and that system owners are communicating changes to impacted groups.

> **Management's Response:** The IRS agreed with this recommendation and will enhance the annual validation process to confirm consistent designation of PII and FTI inventory data across all inventory systems and ensure system owners effectively communicate changes to the relevant groups.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has an effective process to consistently identify systems and applications and track sensitive data held on these systems across multiple inventory systems. To accomplish our objective, we:

- Determined whether the IRS has a standardized process for naming systems and applications by obtaining and analyzing the system naming standards for the ABA, the FISMA Master Inventory, the PIAMS, and the ESAT Tracker.
- Determined whether the IRS has a standardized process to consistently identify systems and applications across its multiple inventory systems by comparing 176 systems included in the FISMA Master Inventory with the ABA, the PIAMS, and the ESAT Tracker inventory reports and identifying missing systems or systems that were inconsistently named.
- Determined whether the IRS consistently identified systems containing sensitive types of data (*i.e.*, PII and FTI) across its inventory systems by comparing the PII and FTI designation for each system across the FISMA Master Inventory, the PIAMS, and the ESAT Tracker inventory reports. We selected all 59 IRS systems that track PII and FTI and were consistently named across the 3 inventory reports, the FISMA Master Inventory, the PIAMS, and the ESAT Tracker.

Performance of This Review

This review was performed with information obtained from the Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland, and the Privacy, Governmental Liaison and Disclosure Office located at the IRS Headquarters in Washington, D.C., during the period October 2023 through October 2024. 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 the data obtained from the ABA, the PIAMS, the ESAT Tracker, the FISMA Master Inventory, the Treasury FISMA Inventory Management System, and the IRS user access system report. We evaluated the data by 1) interviewing IRS personnel knowledgeable about the data; 2) ensuring that the information was legible and contained alphanumeric characters; 3) reviewing required data elements; and 4) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data. We determined that the data from the ABA, the FISMA Master Inventory, the PIAMS, the ESAT Tracker, and the Treasury FISMA Inventory Management System were sufficiently reliable for purposes of this report. For inventory report analysis, we used the data in the FISMA Master Inventory instead of the data in the Treasury FISMA Inventory Management System because the formatting of the data was more closely aligned to the other inventory reports. According to the IRS, the IRS user access system report data was not reliable.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Office of Management and Budget and National Institute of Standards and Technology guidance, and Internal Revenue Manual policies. We evaluated these controls by interviewing IRS subject matter experts, comparing relevant inventory data, and reviewing program and system documentation.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 82 systems in the FISMA Master Inventory that were not consistently named (see Recommendations 2 and 3).

Methodology Used to Measure the Reported Benefit:

We compared 176 systems included in the FISMA Master Inventory as of December 2023 with the ABA, the PIAMS, and the ESAT Tracker inventory reports. We determined that 82 systems across the required inventory reports were named inconsistently.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 11 systems that were not documented in inventory reports as required (see Recommendations 2 and 3).

Methodology Used to Measure the Reported Benefit:

We compared 176 systems included in the FISMA Master Inventory as of December 2023 with the ABA, the PIAMS, and the ESAT Tracker inventory reports. During our efforts to reconcile the differences, we determined that 11 FISMA Master Inventory systems should have been added to the ABA, the PIAMS, and/or the ESAT Tracker inventory systems.

Type and Value of Outcome Measure:

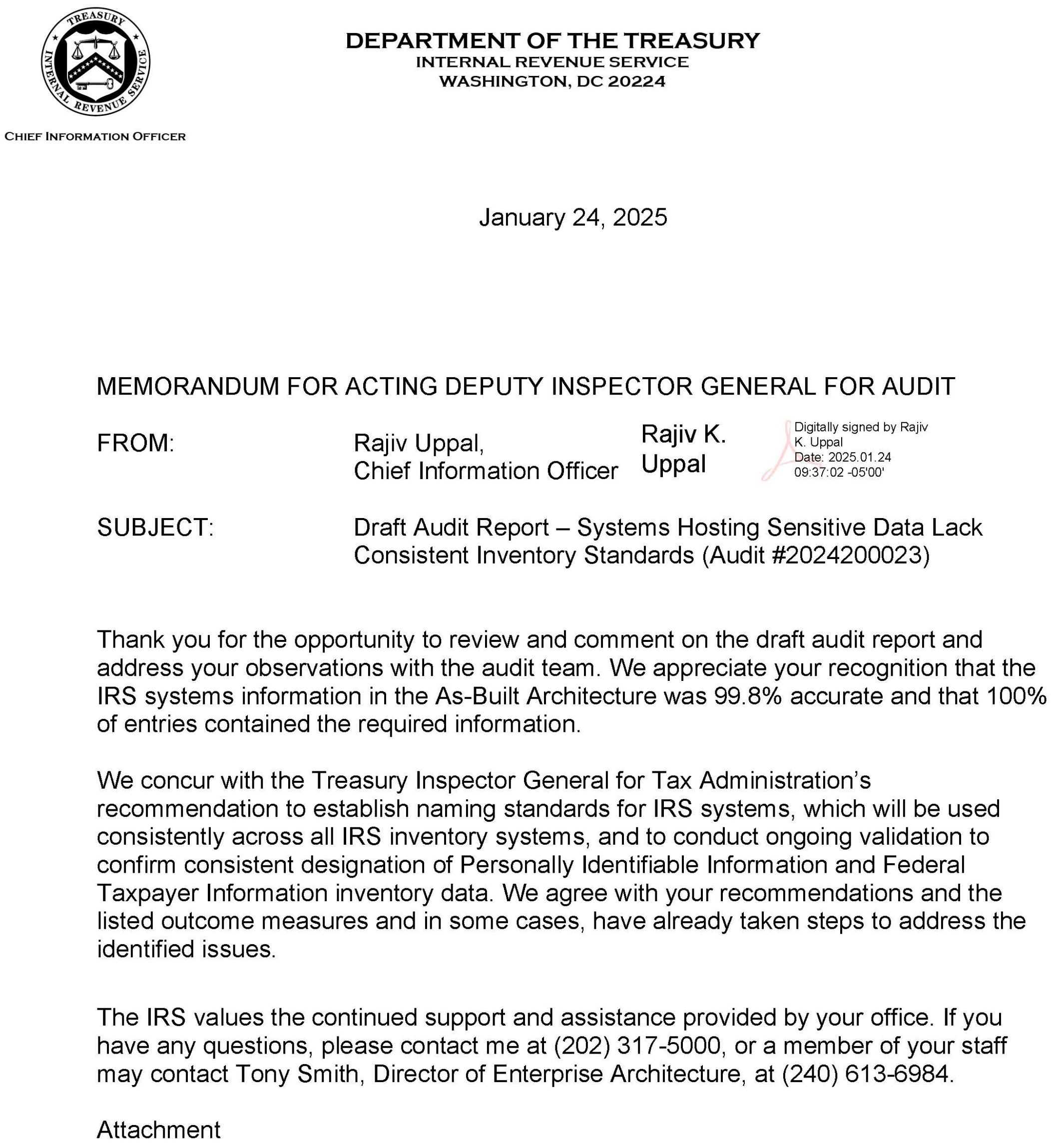
- Reliability of Information – Potential; seven systems containing sensitive data that were not consistently designated across three inventory systems (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

We compared all 59 systems that were consistently named across the 3 inventory reports that track systems containing PII and FTI, the FISMA Master Inventory, the PIAMS, and the ESAT Tracker. We determined that seven systems containing PII and FTI were not consistently designated across the multiple inventory systems.

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

January 24, 2025

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal,
Chief Information Officer

Rajiv K. Uppal

Digitally signed by Rajiv K. Uppal
Date: 2025.01.24 09:37:02 -05'00'

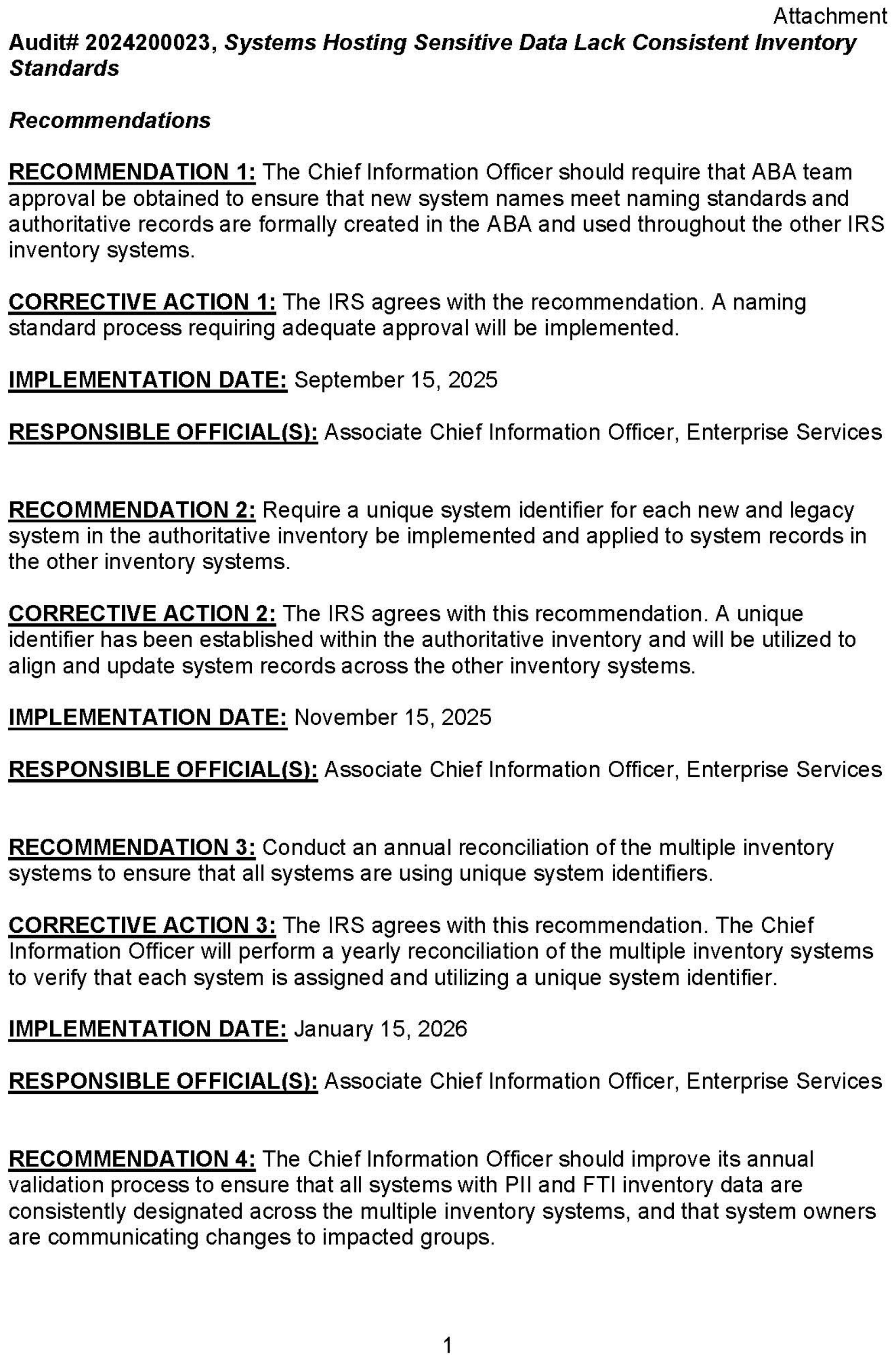
SUBJECT: Draft Audit Report – Systems Hosting Sensitive Data Lack Consistent Inventory Standards (Audit #2024200023)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. We appreciate your recognition that the IRS systems information in the As-Built Architecture was 99.8% accurate and that 100% of entries contained the required information.

We concur with the Treasury Inspector General for Tax Administration's recommendation to establish naming standards for IRS systems, which will be used consistently across all IRS inventory systems, and to conduct ongoing validation to confirm consistent designation of Personally Identifiable Information and Federal Taxpayer Information inventory data. We agree with your recommendations and the listed outcome measures and in some cases, have already taken steps to address the identified issues.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Tony Smith, Director of Enterprise Architecture, at (240) 613-6984.

Attachment



Attachment

Audit# 2024200023, *Systems Hosting Sensitive Data Lack Consistent Inventory Standards*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should require that ABA team approval be obtained to ensure that new system names meet naming standards and authoritative records are formally created in the ABA and used throughout the other IRS inventory systems.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. A naming standard process requiring adequate approval will be implemented.

IMPLEMENTATION DATE: September 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 2: Require a unique system identifier for each new and legacy system in the authoritative inventory be implemented and applied to system records in the other inventory systems.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. A unique identifier has been established within the authoritative inventory and will be utilized to align and update system records across the other inventory systems.

IMPLEMENTATION DATE: November 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 3: Conduct an annual reconciliation of the multiple inventory systems to ensure that all systems are using unique system identifiers.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will perform a yearly reconciliation of the multiple inventory systems to verify that each system is assigned and utilizing a unique system identifier.

IMPLEMENTATION DATE: January 15, 2026

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 4: The Chief Information Officer should improve its annual validation process to ensure that all systems with PII and FTI inventory data are consistently designated across the multiple inventory systems, and that system owners are communicating changes to impacted groups.

Attachment

Audit# 2024200023, *Systems Hosting Sensitive Data Lack Consistent Inventory Standards*

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will enhance the annual validation process to confirm consistent designation of PII and FTI inventory data across all inventory systems and ensure system owners effectively communicate changes to the relevant groups.

IMPLEMENTATION DATE: March 15, 2026

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

Appendix IV

Glossary of Terms

Term	Definition
As-Built Architecture	The authoritative source of the IRS's information technology and business environments. It documents the production environment of IRS systems, infrastructure, technology platforms, *etc*.
Classification	A systematic arrangement in groups or categories according to established criteria.
Enterprise Security Audit Trails	A security auditing tool that allows the collection, retention, and review of enterprise security audit events.
Federal Tax Information	Consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Inventory	A detailed list of assets.
One Solution Delivery Life Cycle	A single delivery model for information technology projects within the IRS.
Privacy and Civil Liberties Impact Assessment	An analysis of how information in an identifiable form is collected, stored, protected, shared, and managed. The process also provides a means to assure compliance with all applicable laws and regulations governing taxpayer and employee privacy.
Privacy Impact Assessment Management System	The IRS's central repository for all privacy impact assessments.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. It normally includes hardware, software, information, data, applications, communications, and people.

Appendix V

Abbreviations

ABA	As-Built Architecture
ESAT	Enterprise Security Audit Trails
FISMA	Federal Information Security Modernization Act of 2014
FTI	Federal Tax Information
IRS	Internal Revenue Service
One SDLC	One Solution Delivery Life Cycle
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information
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 www.tigta.gov/form/suggestions.

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