TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities

September 2, 2025

Report Number: 2025-200-038

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

HIGHLIGHTS: The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities

Final Audit Report issued on September 2, 2025 **Report Number 2025-200-038**

Why TIGTA Did This Audit

The IRS uses an asset and vulnerability repository to collect and index data and assist business units in detecting unauthorized and privileged access abuse. The IRS also uses this repository to manage vulnerabilities and configuration compliance.

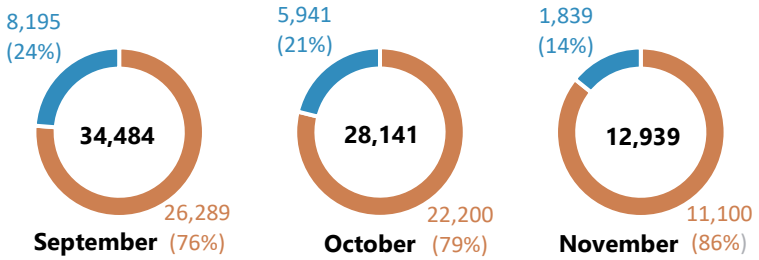
This audit reviewed the vulnerability and configuration compliance of technology assets assigned to the General Support System (GSS) Big Data Analytics (BDA). A GSS is an interconnected set of information resources under the same direct management control which shares common functionality.

Impact on Tax Administration

Federal and organizational policies require the IRS to identify and timely remediate vulnerabilities on its information technology assets and maintain compliance with configuration management and monitoring standards. The existence of unresolved vulnerabilities increases the risk to the overall security of the IRS's information technology assets. Because the GSS BDA contains taxpayer data, it may be exposed to a higher risk of attack.

What TIGTA Found

Overdue and unresolved vulnerabilities increase the risk that information technology assets are not secure. A vulnerability is a weakness in a system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source. Our review of unresolved vulnerabilities in the GSS BDA vulnerability reports from September through November 2024, found that the GSS had fewer unresolved vulnerabilities each month.



However, the percentage of overdue critical vulnerabilities increased from 27 percent to 98 percent during the same period. According to IRS management, the overdue vulnerabilities could not be remediated because of an ongoing upgrade to the operating system of the GSS BDA.

In addition, assets were not properly configured and reported. Our review of Configuration Compliance Tool Dashboard reports found that none of the tracked assets from November 2024 through January 2025 were compliant. IRS management stated that the team prioritized system reboot issues on GSS BDA production systems during a server upgrade that took place from June 2024 to October 2024. The IRS prepared documentation accepting this risk, as required.

Further, the IRS's asset discovery tool, which is used to complete automated screening for assets, was not correctly mapped to the source data. As a result, more than 60 percent of the 919 GSS BDA assets were not reported properly from November 2024 through January 2025.

Finally, our review of the November 2024 vulnerability reports identified 44 GSS BDA assets that were not assigned to the appropriate GSS. Management stated this was caused by a software upgrade.

What TIGTA Recommended

We made three recommendations to the Chief Information Officer, including that GSS BDA vulnerabilities be timely remediated; ensure that all configurations for BDA assets adhere to federal and IRS policies. The IRS agreed with all three recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

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

September 2, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities (Audit No.: 2025200008)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) effectively assigns information technology assets to and addresses security vulnerability issues on the Big Data Analytics General Support System. This review is part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Protection of 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 K. Hung, Acting Assistant General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

The Internal Revenue Service (IRS) uses General Support Systems (GSS) that are an interconnected set of information resources under the same direct management control which shares common functionality. These systems typically include hardware, software, information, data, applications, communications, and people.[1] In addition, the IRS uses Major Applications that require special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. System owners must ensure that the system components are accurately recorded, and system vulnerabilities are identified and remediated timely.

The IRS leverages the asset and vulnerability repository to collect and generate audit records for security-related events. The asset and vulnerability repository:

- Helps individual business units and projects to detect unauthorized intrusions and privileged access abuse.
- Collects and indexes machine data from physical, virtual, or cloud environments that can be used for security, configuration compliance, fraud detection, infrastructure, operational management, and for application delivery and quality assurance.
- Contains vulnerability reports for temporary (a place holder for new assets added to the network that do not have a predefined GSS) and unknown (assets in which the GSS field is blank) information technology assets.
- Tracks 21 different GSSs and Major Applications and identifies a point of contact and responsible organization for each system.

Reports help monitor the status of resolving vulnerabilities

Vulnerability reports contain identifiers to document the status of the vulnerability resolution such as the severity of the vulnerability and the number of days a vulnerability has affected an asset. A vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Vulnerabilities are measured using the Common Vulnerability Scoring System, created by the National Institute of Standards and Technology (NIST). The NIST uses a quantitative methodology to assign a numerical score between 0.0 to 10.0 to a vulnerability to determine its severity. See Figure 1 for the vulnerability scoring table.

[1] See Appendix IV for a glossary of terms.

Figure 1: The National Institute of Standards and Technology Vulnerability Scoring System

Common Vulnerability Scoring System	Vulnerability Severity
0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Source: The Internal Revenue Manual.

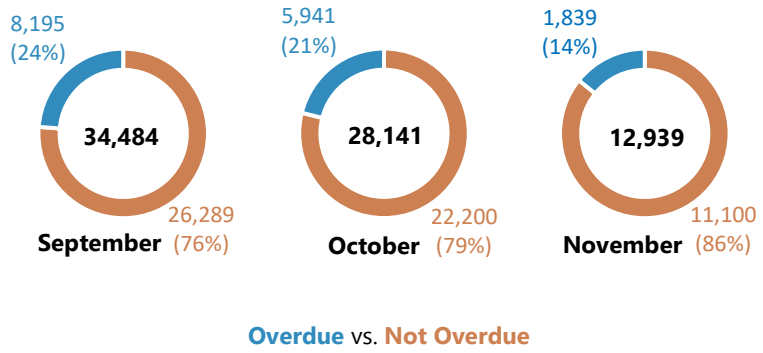
Results of Review

Overdue and Unresolved Vulnerabilities Increase the Risk that Information Technology Assets Are Not Secure

The GSS Big Data Analytics (BDA) (herein referred to as the GSS BDA) is a combination of physical servers and appliance-based infrastructure that provides the ability to conduct advanced analytics and in-depth data analysis of large volumes of data with minimal delay. The GSS BDA performs high-speed data processing that facilitates IRS audit selections and analyzes tax return data.

Our review of unresolved vulnerabilities in the GSS BDA vulnerability reports from September through November 2024 found a reduction in the total of unresolved vulnerabilities each month. However, the severity of the vulnerabilities that were not mitigated within the required time frames, *i.e.*, overdue, increased. Figure 2 summarizes the number of unresolved and overdue vulnerabilities from September through November 2024.

Figure 2: Unresolved and Overdue GSS BDA Vulnerabilities



Source: Analysis of vulnerability reports from the IRS asset and vulnerability repository.

We also reviewed the November 2024 vulnerability and asset repository reports to determine the severity level of all overdue vulnerabilities for 206 GSS BDA assets. Our review shows that despite the reduction in total vulnerabilities, the percentage of overdue critical vulnerabilities increased from 27 percent in September 2024 to 98 percent in November 2024. Although the IRS reduced the total overdue vulnerabilities each month through its remediation process; a significant number of overdue critical risk vulnerabilities remain each month. Critical vulnerabilities can be more difficult to address because fixing one vulnerability can sometimes either introduce new vulnerabilities or negatively impacting existing functionalities. Figure 3 summarizes the total number and the severity level of overdue vulnerabilities from September through November 2024.

Figure 3: Percentage of Overdue Critical and High Risk Vulnerabilities Are Consistently Over 85 percent

	September 2024[2]		October 2024		November 2024	
Critical Risk	2,174	27%	4,761	80%	1,794	98%
High Risk	5,054	62%	876	15%	43	2%
Medium Risk	967	12%	304	5%	2	0%
Total Overdue Vulnerabilities	8,195		5,941		1,839	

Source: Analysis of vulnerability reports from the IRS asset and vulnerability repository.

Finally, we compared all unresolved vulnerabilities from September through November 2024 against the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) Catalog.[3] We found one high risk KEV affecting one asset in September 2024, that was not resolved until November 2024. KEVs are weaknesses in software, hardware, applications, or systems that are being actively exploited by attackers. KEVs offer attackers a proven path to gain access to systems. As such, this vulnerability was susceptible to exploitation by a bad actor for almost two months.

The Enterprise Services function follows NIST and Internal Revenue Manual (IRM) policies for vulnerability remediation to safeguard GSS BDA assets.[4] According to the IRM, the IRS must:

- Monitor and scan for vulnerabilities in the system and hosted applications.
- Analyze vulnerability scan reports and results and remediate vulnerabilities in accordance with response times, prioritizing those with the highest risk. See the time frames outlined in Figure 4.

[2] Percentage totals do not equal 100 percent due to rounding.

[3] The KEV catalog is a Cybersecurity Infrastructure Security Agency maintained list of vulnerabilities that have been previously exploited.

[4] National Institute of Standards and Technology, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

Figure 4: Remediation Timelines

Risk Level	Remediate Vulnerability
Critical	• Internet accessible systems identified in Department of Homeland Security, Cyber Hygiene Reports = 15 days • All other systems = 30 days
High	• Internet accessible systems identified in Department of Homeland Security, Cyber Hygiene Reports = 30 days • High value assets = 60 days • All other systems = 90 days
Medium	• 120 days
Low	• 180 days

Source: The Internal Revenue Manual.

If a vulnerability cannot be effectively remediated within the required time frames, the system's owner must document the vulnerability in a Risk-Based Decision or Plan of Action and Milestones. We did not identify any Risk Based Decisions or Plan of Action and Milestones related to address the unresolved vulnerabilities we found.

According to IRS management, the overdue vulnerabilities could not be remediated because of an ongoing upgrade to the operating system of the GSS BDA. Remediation activity is paused until the operating system upgrade is complete and the team can assess next steps for the remaining vulnerabilities. We previously reported similar concerns about the IRS not timely remediating vulnerabilities in August 2023 and September 2024.[5] The existence of unresolved vulnerabilities increases the risk to the overall security of the IRS's information technology assets. Because the GSS BDA contains taxpayer data, it may be exposed to a higher risk of attack.

Recommendation 1: The Chief Information Officer should timely remediate GSS BDA vulnerabilities in accordance with IRS policies.

Management's Response: The IRS agreed with this recommendation and will ensure the Managed Service Provider remediates all GSS BDA vulnerabilities in accordance with IRS policy and will document any unresolved vulnerabilities in a Risk-Based Decision or Plan of Action and Milestone.

Assets Were Not Properly Configured or Reported

Configuration management is a process used to maintain a desired state on information technology systems and components. It helps ensure that accurate information is available for

[5] TIGTA, Report No. 2023-20-048, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk* (August 2023), and TIGTA, Report No. 2024-200-057, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement* (September 2024).

the systems and components. The IRS has established enterprise-wide policies for configuration management and monitoring to ensure that it is following both NIST and IRM requirements. In addition, Enterprise Services personnel have processes to monitor and evaluate the configuration management reports for deficiencies. However, actions have not been taken to address noncompliant and improperly reported assets for November 2024 through January 2025.

BDA assets were not properly configured from November 2024 through January 2025

We reviewed the IRS's Configuration Compliance Tool Dashboard reports for GSS BDA assets from November 2024 through January 2025 and found that none of the tracked assets were properly configured, *i.e.*, noncompliant, during that period.[6] Specifically:

- All 348 tracked assets were noncompliant in November 2024.
- All 64 tracked assets were noncompliant in December 2024.
- All 337 tracked assets were noncompliant in January 2025.

Further assessment of the data shows that over 90 percent of all noncompliant configurations have at least one failed high-severity finding. This means there is at least one vulnerability that poses risk to the information technology asset, the exploitation of which could lead to serious consequences like a full system compromise, access to sensitive data, or significant business disruption. According to the Dashboard User Guide, configuration compliance is achieved when a system reaches a certain compliance score and does not include any high-severity findings.

Enterprise Services management confirmed that all the tracked assets we identified were noncompliant. They explained this occurred because the team prioritized system reboot issues on GSS BDA production systems during a server upgrade that took place from June 2024 to October 2024. The team prepared a Risk-Based Decision for each failed high severity finding and is working on a compliance plan to address the remaining noncompliant assets. Nonetheless, the existence of failed high-severity findings increases the risk to the overall security of the IRS's information technology assets.

Recommendation 2: The Chief Information Officer should ensure that all configurations for GSS BDA assets adhere to federal and IRS policies.

Management's Response: The IRS agreed with this recommendation and will ensure all GSS BDA assets are in compliance with federal and IRS policies.

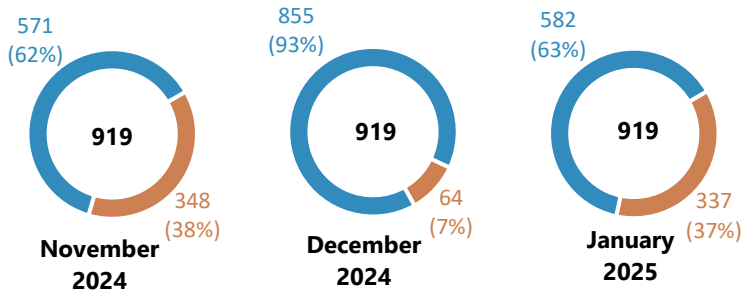
Asset configurations are not properly reported

The IRS provided a list that identified 919 assets assigned to the GSS BDA.[7] We compared the IRS's list of assets to the configuration scan reports and found that over 60 percent of the GSS BDA assets were not accounted for each month. Figure 5 summarizes the number of GSS BDA assets not properly reported between November 2024 and January 2025.

[6] The number of tracked assets may be impacted by the issues with the IRS's asset discovery tool discussed later in this report.

[7] This list included assets from November 2024 through January 2025.

Figure 5: GSS BDA Assets Not Properly Reported



Source: Analysis of configuration compliance reports from the IRS asset and vulnerability repository.

The IRM requires automated security scanning of assets every 30 days. The IRS uses the asset discovery tool to complete its automated security screening of assets. However, according to IRS personnel, the IRS's asset discovery tool was not correctly mapped to the source data. As a result, the asset discovery tool was not populating the critical information for many assets. A service ticket was submitted in November 2024 and the IRS reported the issue was fixed in February 2025. However, our analysis of the May 2025 configuration scan report confirmed that the issue is still occurring.

Recommendation 3: The Chief Information Officer should ensure the asset discovery tool is properly configured to the source data to accurately account for all GSS BDA assets.

Management's Response: The IRS agreed with this recommendation and will ensure the asset discovery tool is properly configured to the source data to accurately account for all GSS BDA assets.

Assets Were Not Assigned to the Appropriate General Support System

IRS policy requires that systems must contain inventory data, such as platform and type, and specify the GSS the data belongs to. Our review of the November 2024 vulnerability reports from the IRS's asset data repository found 44 GSS BDA assets that were listed on the GSS-Unknown report. The GSS-Unknown report identifies assets where there is no entry in the GSS field. IRS management agreed with what we found noting that these errors were caused by a software upgrade in September 2024. The IRS is currently working to develop and test a viable solution that will fix the errors caused by the software upgrade. Assets with missing GSS data significantly increases the risk of asset compromise due to management being unfamiliar with the needs of those assets.

Some individual assets were in multiple vulnerability reports

IRS policy also states that the agency must develop and document an inventory of IRS system components that accurately reflects the system and includes all components within the system.

The inventory must not include duplicate accounting of components or components assigned to any other system.

We reviewed an enterprise level report of affected assets collected in October 2024. This report documents the asset name, Internet Protocol address of the assets, the assigned GSS, and the number of vulnerabilities for each asset grouped by severity. This listing contained approximately 291,000 technology assets. Our review found 5,860 (2 percent) that were assigned to more than one GSS.

- 5,842 assets are shared between a known GSS and the Unknown GSS repository.
- 18 assets are shared between at least two known GSS groups.

The remaining 285,149 (98 percent) technology assets were appropriately assigned to one GSS.

A management official from the Cybersecurity function stated that depending on the type of scan performed, the data will not show the same results. For example, an agent scan will show the assigned GSS for a specific asset, while a different type of scan may not include the GSS in its report. Assets found in more than one GSS calls into question the overall accountability for asset assignment. We previously recommended that the Chief Information Officer should reconcile assets to reflect the operating environment.[8] The IRS plans to take corrective actions to address this recommendation by November 2025. As a result, we are not making another recommendation.

[8] TIGTA, Report No. 2024-200-057, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement*, (September 2024).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the IRS effectively assigns information technology assets to and addresses security vulnerability issues on the BDA GSS. To accomplish our objective, we:

- Assessed the IRS's asset and vulnerability repository by determining whether assets were assigned to temporary or unknown GSSs and if assets are assigned to multiple GSSs or major applications.
- Determined if the IRS remediated vulnerabilities timely by assessing vulnerability data and reviewing vulnerability scan reports.
- Evaluated the vulnerability remediation process and procedures for assigning assets to BDA by interviewing Enterprise Services and Cybersecurity function personnel and reviewing documented policies and procedures.
- Determined the IRS's compliance with federal and agency configuration requirements by reviewing asset configuration data and configuration compliance reports.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity and Enterprise Services functions located in the New Carrollton Federal Building in Lanham, Maryland during the period October 2024 through February 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 obtained data directly from the asset and vulnerability repository. We completed data reliability assessments to ensure that the data were sufficiently reliable to use to complete our audit objectives. We evaluated data from the asset and vulnerability repository from September 2024 through January 2025. We compared similar data elements and validated the data reports to ensure that the information was accurate by discussing the results with IRS management and making comparisons with the asset inventory data to determine its reasonableness. 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: processes, policies, procedures, and guidelines related to the management of information technology assets, vulnerability resolution, and configuration management. We evaluated these controls by interviewing Information Technology organization personnel and analyzing the IRS's asset, vulnerability, and configuration repositories.

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:

Protection of Resources – Potential; 206 assets from a GSS BDA vulnerability report that were unresolved and overdue (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We analyzed the complete population of asset vulnerabilities in November 2024. We determined that the GSS BDA vulnerability report contains 206 assets that remain unresolved past the remediation window determined by IRS policy. As a result, the asset protection is compromised, and the risk to the overall security of IRS assets persists.

Type and Value of Outcome Measure:

Protection of Resources – Potential; 337 GSS BDA assets that were operating with noncompliant configuration baselines (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We reviewed the IRS Configuration Compliance Tool Dashboard January 2025 report for GSS BDA assets and found that 337 GSS BDA assets contain configurations that were noncompliant. As a result, the asset protection is compromised, and the risk to the overall security of IRS assets persists.

Type and Value of Outcome Measure:

Reliability of Information – Potential; 582 GSS BDA assets that were not properly reported (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We compared the GSS BDA list of assets to the configuration scans from November 2024 through January 2025. We found that the January 2025 configuration scan tracked 337 assets, and the GSS BDA list contained 919 assets. There were 582 (919-337) assets that did not show a configuration status. However, according to IRS personnel, the IRS's asset discovery tool was not correctly mapped to the source data. As such, the asset discovery tool was not populating the critical information for many assets. As a result, reliability of the configuration reporting data is called to question.

Appendix III

Management's Response to Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

August 5, 2025

MEMORANDUM FOR DIANA M. TENGESDAL
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Chief Information Officer
Courtney M. Williams
Digitally signed by Courtney M. Williams
Date: 2025.08.05 22:12:52 -04'00'

SUBJECT: Draft Audit Report – The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities (Audit #2025200008)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. The IRS appreciates opportunities to improve internal controls and oversight processes and is committed to providing oversight of the Managed Service Provider (MSP) to ensure the resolution of the items addressed in the audit report.

The IRS agrees with the Treasury Inspector General for Tax Administration's recommendations and associated outcome measures addressed in the report. We have already begun working to implement these measures with the MSP to address overdue and unresolved vulnerabilities on the Big Data Analytics platform. Since the issuance of this report, the MSP has delivered measured improvement and continues to work toward the timely mitigation of critical vulnerabilities.

Our corrective action plan for the three recommendations and outcome measures identified in the report is attached.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact me at (304) 616-1818, or a member of your staff may contact Rob King, Coordinating Director, API Layer & Platform Engineering, at (469) 801-1202.

Attachment

Attachment
Audit #2025200008, The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities

Recommendations

RECOMMENDATION 1: The Chief Information Officer should timely remediate GSS BDA vulnerabilities in accordance with IRS policies.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will ensure the Managed Service Provider remediates all GSS BDA vulnerabilities in accordance with IRS policy and will document any unresolved vulnerabilities in a Risk-Based Decision or Plan of Action and Milestone.

IMPLEMENTATION DATE: September 15, 2025

RESPONSIBLE OFFICIAL(S): Coordinating Director, API Layer & Platform Engineering

RECOMMENDATION 2: The Chief Information Officer should ensure that all configurations for GSS BDA assets adhere to federal and IRS policies.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will ensure all GSS BDA assets are in compliance with federal and IRS policies.

IMPLEMENTATION DATE: February 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, API Layer & Platform Engineering

RECOMMENDATION 3: The Chief Information Officer should ensure the asset discovery tool is properly configured to the source data to accurately account for all GSS BDA assets.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will ensure the asset discovery tool is properly configured to the source data to accurately account for all GSS BDA assets.

IMPLEMENTATION DATE: April 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Asset	A major application, general support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.
Agent Scan	A low-footprint program that installs locally on hosts.
Configuration Management	Establishes proper control over approved project documentation, hardware, and software, and assures changes are authorized, controlled, and tracked.
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, relating to progress and performance.
Enterprise Services	An IRS function responsible for strengthening technology infrastructure across the enterprise.
High Value Assets	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical federal operations or house unique collections of data (by size or content) making them of particular interest to criminal, politically motivated, or state sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Internal Revenue Manual	The primary source of instructions to employees relating to the administration and operation of the IRS. The IRM contains the directions employees need to carry out their operational responsibilities.
Internet Protocol Address	The standard protocol for transmission of data from source to destination in packet-switched communications networks and interconnected systems such as networks.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Severity Rating	One of five levels on a ratings scale to describe the risk associated with a vulnerability. The complete scale from lowest risk to highest risk is: Informational, Low, Medium, High, and Critical.

Term	Definition
Vulnerability	A weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.

Appendix V

Abbreviations

BDA	Big Data Analytics
GSS	General Support System
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
KEV	Known Exploited Vulnerability
NIST	National Institute of Standards and Technology
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.