TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration

September 17, 2024

Report Number: 2024-200-048

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

HIGHLIGHTS: Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration

Final Audit Report issued on September 17, 2024 **Report Number 2024-200-048**

Why TIGTA Did This Audit

The IRS is entrusted with protecting information received from taxpayers, including Personally Identifiable Information and tax account data. The IRS's Data Loss Prevention (DLP) solution is designed to detect and prevent the inadvertent or deliberate transfer of sensitive data outside of the IRS network.

This audit was initiated to evaluate the IRS's controls to prevent the exfiltration of sensitive taxpayer data.

Impact on Tax Administration

As the Nation's tax agency, the IRS collects and stores substantial amounts of Personally Identifiable Information, including all tax records for individuals and corporations. In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases.

There are [redacted] potential methods for data exfiltration from within the IRS, [redacted] Data exfiltration is typically caused by an outsider attack, a careless inadvertent insider threat, or in some cases a malicious insider threat.

The successful exfiltration or removal of taxpayer data for unauthorized purposes could erode public trust in the IRS's ability to administer our Nation's tax system.

What TIGTA Found

The IRS is monitoring data and collecting metrics for all three DLP solution components. TIGTA reviewed the metrics used by the IRS to measure the various DLP components' efficacy and determined that a DLP tool was in place.

The IRS implemented a network visibility tool to identify and track unauthorized access attempts to external connections. However, the IRS controls [redacted] using secure connections. During our testing, TIGTA determined that the IRS network allowed the [redacted] of mock, *i.e.*, simulated, taxpayer data to a [redacted] Also, the IRS controls [redacted] of taxpayer data to [redacted] The IRS network allowed the [redacted] of mock taxpayer data to [redacted]

In addition, the IRS has controls in place to monitor and prevent [redacted] taxpayer data [redacted] through [redacted] but the solution [redacted] and is [redacted] taxpayer information and [redacted] types. These [redacted] for the potential intentional exfiltration of taxpayer data by [redacted] outside of the IRS.

The IRS has controls in place to limit and monitor the use of [redacted] All IRS users who had the ability to [redacted] also had the required approval. However, the approval process was not always followed, and [redacted] percent) of [redacted] sampled users were provided with [redacted] access to [redacted] without providing adequate justifications.

Finally, the IRS is effectively preventing users from using [redacted] and has controls in place to [redacted] sensitive data transmitted to [redacted]

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer, in conjunction with the Chief Operating Officer, should: (1) implement more prohibitive controls for allowing users to transfer information [redacted] (2) revise the DLP rules to be more restrictive to help prevent intentional data exfiltration; and (3) continue to ensure that the managers and executives responsible for approving [redacted] access carefully review all requests and approve only those with sufficient and appropriate responses.

The IRS agreed with all three recommendations. The Chief Information Officer and Chief Operating Officer plan to review existing controls and policy to [redacted] review the rules and policy within the DLP tool and implement additional rules or controls to improve data security; and enhance communication for approvers of [redacted] requests to focus on business needs justifications.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 17, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration (Audit No.: 202320025)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) controls to prevent the exfiltration of sensitive taxpayer data. This review is included in our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenges of *Protection of Taxpayer Data and IRS Resources* and *Information Technology Modernization*.

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

Table of Contents

Background

The Internal Revenue Service (IRS) is entrusted with protecting information received from taxpayers, including Personally Identifiable Information (PII) and tax account data.[1] As the Nation's tax agency, the IRS collects and stores substantial amounts of PII, including all tax records for individuals and corporations. In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases. Allowing this information to be removed or exfiltrated for unauthorized purposes could erode public trust in the IRS's ability to administer our Nation's tax system and in the voluntary compliance nature of tax filing. To address this risk, the IRS implemented a Data Loss Prevention (DLP) solution. This solution is designed to detect and prevent the inadvertent or deliberate transfer of PII outside the IRS network.

The IRS Cybersecurity Architecture and Implementation's Cybersecurity Information Protection Enhancement Controls Program, which is responsible for implementing the DLP solution, started in Calendar Year 2010.[2] The project team implemented and expanded the Data-in-Motion component of the solution that includes [redacted] for the [redacted] PII used by the IRS.

Despite the DLP solution, in November 2020, an IRS contractor disclosed tax information without authorization. Through data exfiltration, the contractor stole tax return information for thousands of the U.S.'s wealthiest individuals and disclosed it to a news organization. Data exfiltration (or data theft) is the intentional, unauthorized, covert transfer of data from a computer or other device. There are several potential methods for data exfiltration from within the IRS, [redacted]. Data exfiltration is typically caused by an outsider attack, a careless inadvertent insider threat, or in some cases a malicious insider threat. While intentional insider threats may be a smaller segment of the data exfiltration incidents, it is an important security risk, and the focus of this audit.

Results of Review

The IRS Is Monitoring Data and Collecting Metrics for All Three Data Loss Prevention Solution Components

The IRS stated that it has implemented all three components of the DLP Solution: Data-In-Motion, Data-in-Use, and Data-at-Rest.

- The Data-in-Motion component monitors and blocks outbound [redacted] transmissions containing unprotected sensitive data.

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

[2] Previously called the Safeguarding PII Data Extracts Project.

- The Data-in-Use component detects and monitors unprotected outbound sensitive data transmissions via [redacted] methods, [redacted] and provides a warning to users if they are about to [redacted] unprotected sensitive data by [redacted]
- The Data-at-Rest component scans stored IRS data for unprotected sensitive data.

We reviewed the metrics used by the IRS to measure the various DLP components' efficacy and determined that a DLP tool was in place. Figure 1 provides the number of incidents for each component for Calendar Years 2022 and 2023.

Figure 1: Data Loss Prevention Incidents

Calendar Year	Data-In-Motion [redacted] Incidents	Data-in-Use Incidents [redacted]	Data-at-Rest Incidents
2022	88,254	139,678	122,211
2023	95,491	158,077	191,166

Source: IRS Cybersecurity Information Protection Enhancement Controls Program.

The National Institute of Standards and Technology (NIST) recommends that agencies implement automated tools to monitor PII internal network boundaries for unusual or suspicious transfers or events.[3]

The IRS Has Controls to Prevent the Exfiltration of Data; but, [redacted]

The NIST states that the prevention of data exfiltration applies to both the intentional and unintentional exfiltration of information. We reviewed the IRS's controls over several areas that could be used to intentionally exfiltrate data [redacted] We used mock, *i.e.*, simulated, taxpayer data comprised of [redacted]

Controls are in place to detect, monitor, and sever external connections; however, [redacted]

The IRS implemented a network visibility tool to identify and track unauthorized access attempts to [redacted] We reviewed the tool and determined it has capabilities such as real-time monitoring, detecting malicious activities, and blocking unauthorized access. However, the controls to [redacted] external connections [redacted] mock taxpayer data [redacted] The NIST requires organizations to detect and deny outgoing communications traffic posing a threat to systems and audit the identity of internal users associated with denied communications.

[3] NIST, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (Sept. 2020).

[redacted]

We [redacted] to attempt to exfiltrate mock taxpayer data. We established a [redacted] accessed it through an IRS virtual machine, and [redacted] mock taxpayer data [redacted]

[redacted]

The IRS allows users to access [redacted] We [redacted] to determine if the IRS network would [redacted] of sensitive taxpayer data. Our testing of mock taxpayer data determined that the IRS network allowed uploads of taxpayer data to [redacted]

The Internal Revenue Manual (IRM) states that users cannot post or upload PII and tax information online, unless secured with Information Technology-approved access controls by the IRS.[4] It also states that such data may be reproduced only to the extent needed to carry out official business. In addition, the IRM requires the electronic transmission of tax information to be encrypted for security purposes. The IRS does not always [redacted] access to [redacted] accessible on [redacted] users can exfiltrate taxpayer data.

Recommendation 1: The Chief Information Officer, in conjunction with the Chief Operating Officer, should implement more prohibitive controls for allowing users to [redacted]

Management's Response: The IRS agreed with this recommendation. The Data Security Executive Steering Committee, which includes the Chief Operating Officer and Chief Information Officer as members, plans to review existing controls and policy in place to [redacted]
The Chief Operating Officer plans to ensure that the new controls and policies are approved by all stakeholders. The Chief Information Officer plans to implement the additional rules, policy, and controls along with ongoing monitoring and reporting to the Data Security Executive Steering Committee as applicable.

Controls are in place to prevent users [redacted] sensitive taxpayer data; however, [redacted]

The DLP solution monitors [redacted] from the IRS [redacted] system and compares the information contained [redacted] and [redacted] to the established rule sets and [redacted] from transmission if the sensitive taxpayer information [redacted] meets the rules. We attempted [redacted] with mock taxpayer data [redacted] and were successfully [redacted] by the DLP solution.

However, we found that [redacted] to an [redacted] and [redacted] that [redacted] to a [redacted] Once [redacted] was transmitted, we were able to [redacted] open it on a

[4] IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* (Sept. 2023).

personal device, and read the data. In addition, following IRS approved methods for external [redacted] we were able to [redacted] and [redacted] We then were able to [redacted]

The IRM requires users to use IRS approved encryption technology when including any taxpayer data in [redacted].[5] The DLP solution is intended to prevent [redacted] transmission of data that could be intercepted by bad actors. The DLP solution is not designed [redacted] when users follow approved methods for external [redacted] In addition [redacted] information, our testing determined that the DLP rules are [redacted] of taxpayer information. When the taxpayer information is intentionally [redacted] of the DLP solution, [redacted] For example, we [redacted] when we [redacted] the [redacted] an [redacted] and when we [redacted] the [redacted] of the [redacted]

These [redacted] that there are [redacted] the DLP solution that could allow a user to intentionally circumvent the controls and exfiltrate sensitive taxpayer data for inappropriate use. Also, the DLP solution does [redacted] the network when [redacted] its contents.

Recommendation 2: The Chief Information Officer, in conjunction with the Chief Operating Officer, should revise the DLP rules to be more restrictive to help prevent intentional data exfiltration.

Management's Response: The IRS agreed with this recommendation. In coordination with Corrective Action one, the Data Security Executive Steering Committee plans to review existing rules and policy within the DLP tool to [redacted] and identify additional rules or controls to be implemented to improve data security. The Chief Operating Officer plans to ensure that the new controls and policies are approved by all stakeholders. The Chief Information Officer plans to implement the additional rules, policy, and controls along with ongoing monitoring and reporting to the Data Security Executive Steering Committee.

Controls are in place to limit and monitor the use of [redacted]; however, the approval process is not always followed properly

The IRS has a process in place to limit users from [redacted] such as [redacted] To obtain the ability to [redacted] a user must submit a request in the Business Entitlement Access Request System (BEARS) for [redacted] access. Once the manager and executive complete the approval process, BEARS automatically communicates with the Active Directory and adds the user to the group policy that provides the [redacted] access. This automatic communication ensures that permissions are added only when an approval is received. The IRS confirms that users have a continued need by requiring annual approval. The approval is granted from July 1 to June 30.

[5] IRM 1.10.3, *Office of the Commissioner of Internal Revenue,* [redacted] (Nov. 2016).

Employees capable of [redacted] had necessary approval

As of January 26, 2024, the IRS had [redacted] active users with [redacted] approval. We compared these users to a list of all users under the group policy allowing [redacted] access and determined that all users who had the ability to [redacted] also had the required BEARS approval. We also tested the effectiveness of this control [redacted] the computer of an IRS user that did not have the [redacted] approval. The user was able to [redacted] but was unable to [redacted] which demonstrated that the control was working properly. The IRM requires the IRS to restrict the usage of [redacted].[6]

Permission was inappropriately given to users to [redacted]

As part of the approval process the user is required to address four requirements justifying their need:

1. Specific justification and business need.
2. Information that will be [redacted] the system.
3. What will be done with the information [redacted] the system.
4. Document compensating security measure the requester will take to safeguard the data.

We selected a statistically valid random sample of [redacted] users (5 percent) of the [redacted] users with BEARS approvals for [redacted] access.[7] We tested the users' responses to the four required questions to determine if they were valid and the user had a reasonable business need for obtaining [redacted] access. We found that [redacted] percent) of the [redacted] users did not have adequate responses, while [redacted] percent) users did have adequate responses.

- One user provided a generic response to the justification and then provided the same response to all four questions.
- One user provided a response of "Not Applicable" to the fourth question about safeguarding the data.
- One user provided a response of "Data" to the fourth question about safeguarding the data.

We determined that all three of these responses were inadequate and did not provide the manager or executive with an appropriate answer to justify approval of the request. Using the results of our statistical sample, we project that [redacted] users across the population of [redacted] users did not have adequate responses.

In a memorandum dated July 12, 2023, the IRS required executive approval for [redacted] access to [redacted].[8] The memorandum states that managers are expected to oversee compliance for all IRS policies and procedures related to the [redacted] including,

[6] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 2023).

[7] Our sample was selected using a 95 percent confidence interval, 5 percent error rate, and ±5 percent precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total amount is between [redacted] and [redacted].

[8] IRS, *Revised* [redacted] *Procedures* (July 2023).

but not limited to, assessing the continued business need for any exception granted, as well as routinely reinforcing the importance of data protection.

We asked the IRS why the [redacted] users with inadequate answers were granted access. The IRS stated that prior approvals were executed on these users and the executives were asked to re-evaluate prior approvals. The prior approvals may have resulted in some leniency toward the responses. By approving user requests for [redacted] access without ensuring that each user understands the risks inherent in [redacted] sensitive taxpayer information, the IRS risks allowing users who do not have a need [redacted] taxpayer data to exfiltrate the data. In addition, these users may also not sufficiently understand the inherent risks in having data [redacted]

Recommendation 3: The Chief Information Officer, in conjunction with the Chief Operating Officer, should continue to ensure that the managers and executives responsible for reviewing and approving BEARS [redacted] requests carefully review all requests and only approve requests with sufficient and appropriate responses to the required questions.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer, in conjunction with the Chief Operating Officer, plans to enhance communication for approvers of [redacted] requests to focus on sufficient documentation of business needs justifications.

The IRS is effectively preventing users from using [redacted]

The IRS [redacted] The IRS uses a [redacted] lookup tool that categorizes [redacted] and determines if a [redacted] is properly categorized and if not, requests the vendor to categorize the [redacted]. The IRM states that no officer or employee of the IRS may use a [redacted] to conduct any official business of the Government.

We selected a judgmental sample of 50 [redacted] that were [redacted] by the IRS and tested our access to them on an IRS virtual machine.[9] We determined that the IRS properly [redacted] all 50 [redacted]. We also performed our own search on the Internet to develop a list of [redacted] and identified 105 additional [redacted]. We tested all 105 [redacted] to determine if the IRS's [redacted] access. While the [redacted] limited access to the main page for 16 [redacted] and allowed the [redacted] two [redacted] there were no [redacted] on which we were able to [redacted] For the remaining 87, [redacted]

Controls are in place to monitor sensitive data transmitted to [redacted]

The IRS has an [redacted] in place on IRS [redacted] to [redacted] sensitive data that is [redacted] While performing on-site testing at the IRS, we observed an IRS user [redacted] mock taxpayer data to a [redacted] After the data were [redacted] the IRS official provided us with the log that was produced by the [redacted] action. IRS officials explained [redacted] sensitive data [redacted] necessary as part of IRS business operations. While performing tests on-site, the IRS demonstrated that users were required to go to the [redacted] and enter their security credentials before the [redacted] was

[9] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

completed. This ensured that the user was present and able to [redacted] the sensitive data immediately.

We asked the IRS about procedures for the disposal of [redacted] The IRS provided their policy for asset management, sanitization, and disposal.[10] The NIST requires organizations to sanitize media prior to the disposal of digital and non-digital systems, including printers. We reviewed the IRS's policy and determined that it is consistent with NIST requirements.

[10] IRS, *AM063 v2 - Asset Management Policy Directive for Asset Sanitization Prior to Disposal* (Jan. 2022).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the IRS's controls to prevent the exfiltration of sensitive taxpayer data. To accomplish our objective, we:

- Evaluated the overall implementation status of the DLP solution and determined whether the IRS was monitoring data for all three DLP components by meeting with IRS personnel and reviewing metrics received from the Cybersecurity Information Protection Enhancement Controls Program.
- Evaluated BEARS entitlement applications for [redacted] access for [redacted] by reviewing a sample of applications from the BEARS system. We selected and reviewed a statistically valid sample of [redacted] entitlement applications from a population of [redacted] approved user entitlements for [redacted] access to [redacted] We used a statistical sample to allow the results to be projected to the overall population. We relied on the Treasury Inspector General for Tax Administration's contract statistician to verify our sampling methods. We selected our sample using a 95 percent confidence level, a ±5 percent precision, and a 5 percent estimated error rate.
- Evaluated the controls for [redacted] external connections by interviewing IRS personnel, going on-site for a system demonstration, and reviewing system documentation.
- Evaluated the controls over the use of internal IRS [redacted] to transmit sensitive taxpayer data by testing numerous ways to potentially exfiltrate data from an IRS user account on a virtual machine within the IRS network.
- Evaluated the effectiveness of [redacted] by reviewing a sample of [redacted] by the IRS. We selected a judgmental sample of 50 [redacted] from the population of 1,163 [redacted].[1] We selected a judgmental sample because we did not plan to project to the population. These 50 [redacted] were selected for testing because they were representative of the [redacted] the IRS had listed as [redacted] We also tested an additional 105 [redacted] obtained through Internet searches.

Performance of This Review

This review was performed in the Cybersecurity function at the New Carrollton Federal Building in Lanham, Maryland, and with information obtained from the Office of Privacy, Governmental Liaison and Disclosure located in Washington, D.C., during the period August 2023 through July 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.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Major contributors to the report were Jena Whitley, Acting Assistant Inspector General for Audit; Jason McKnight, Director; Kasey Koontz, Audit Manager; Daniel Preko, Audit Manager; Michael Segall, Acting Audit Manager and Lead Auditor; Vanessa Siegning, Auditor; and Komlanvi Komabane, Information Technology Specialist.

Data Validation Methodology

We performed tests to assess the reliability of data from the BEARS and Active Directory. We evaluated the data by: (1) interviewing agency officials knowledgeable about the data, and (2) observing agency officials, via online meetings with screensharing, pull the data from the systems and comparing the spreadsheets received to the actual data in the system. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRM and NIST policies. We evaluated these controls by interviewing Cybersecurity function personnel; reviewing and comparing the IRM and the NIST guidelines; and testing the controls over reviewing [redacted] applications, access to external [redacted] and [redacted]

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 22, 2024

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal,
Chief Information Officer
Rajiv K. Uppal
Digitally signed by Rajiv K. Uppal
Date: 2024.08.22 08:54:11 -04'00'

SUBJECT: Draft Audit Report – Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration (Audit #202320025)

Thank you for the opportunity to review and comment on the draft audit report. The IRS implements the Data Loss Prevention (DLP) program, in addition to a range of other security measures, to protect taxpayer information from unauthorized disclosure. Any improper disclosure of taxpayer information is unacceptable.

The auditors acknowledge that the IRS has implemented all three components of the DLP program and has controls to prevent the exfiltration of data. We appreciate the auditor's recommendations to further strengthen the program. The IRS agrees with the recommendations and has already taken steps to implement the additional improvements. Our corrective action plan is attached.

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 George Contos, Director, Business Planning and Risk Management, at (202) 317-4287.

Attachment

Attachment

Audit# 202320025, Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration

Recommendations

RECOMMENDATION 1: The Chief Information Officer, in conjunction with the Chief Operating Officer, should implement more prohibitive controls for allowing users to transfer information to [redacted]

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Data Security Executive Steering Committee (DSESC), which includes the Chief Operating Officer and Chief Information Officer members, will review existing controls and policy in place to [redacted]
The Chief Operating Officer will ensure the new controls and policies are approved by all stakeholders. The Chief Information Officer will implement the additional rules, policy, and controls along with ongoing monitoring and reporting to the DSESC as applicable.

IMPLEMENTATION DATE: 11/15/2025

RESPONSIBLE OFFICIAL: Office of the Chief Information Officer

RECOMMENDATION 2: The Chief Information Officer, in conjunction with the Chief Operating Officer, should revise the Data Loss Prevention (DLP) rules to be more restrictive to help prevent intentional data exfiltration.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. In coordination with Corrective Action 1, the DSESC will review existing rules and policy within the Data Loss Prevention tool to [redacted] and identify additional rules or controls to be implemented to improve data security. The Chief Operating Officer will ensure the new controls and policies are approved by all stakeholders. The Chief Information Officer will implement the additional rules, policy, and controls along with ongoing monitoring and reporting to the DSESC.

IMPLEMENTATION DATE: 11/15/2025

RESPONSIBLE OFFICIAL: Office of the Chief Information Officer

RECOMMENDATION 3: The Chief Information Officer, in conjunction with the Chief Operating Officer, should continue to ensure that the managers and executives responsible for reviewing and approving BEARS [redacted] requests carefully review all requests and only approve requests with sufficient and appropriate responses to the required questions.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer, in conjunction with the Chief Operating Officer, will enhance communication for approvers of [redacted] requests to focus on sufficient documentation of business needs justifications.

IMPLEMENTATION DATE: **10/15/2024**

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Appendix III

Glossary of Terms

Term	Definition
Active Directory	A domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. Active Directory also enables administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization simultaneously from a central, organized, accessible database.
Business Entitlement Access Request System	A means to request and document user access to systems/applications.
Data-at-Rest	Data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.
Data-in-Motion	Data moving between systems or devices.
Data-in-Use	Data that is being processed, accessed, or read.
Data Loss Prevention	The practice of detecting and preventing confidential data, such as PII, from being "leaked" out of an organization's boundaries, either intentionally or unintentionally.
Decrypt	The process of converting encrypted data into recognizable information.
Encrypt	The process of converting plain text to cipher text by means of a cryptographic system.
Group Policy	A virtual collection of policy settings.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of PII are name, Social Security Number, date of birth, place of birth, address, and biometric record.
Proxy Server	A server that filters and evaluates each Internet address and request when a user accesses a file or opens a web page.
Solution	An implementation of people, processes, information, and technologies in a distinct system to support a set of business or technical capabilities that solve one or more business problems.
Virtual Machine	A simulated environment created by virtualization, also described as a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer.
Website	A collection of webpages grouped together using the same domain name and operated by the same person or organization.
Zip File	A file that contains one or more compressed files.

Appendix IV

Abbreviations

BEARS	Business Entitlement Access Request System
DLP	Data Loss Prevention
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information

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

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

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