TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Cybersecurity Data Warehouse Needs Improved Security Controls

June 21, 2018

Reference Number: 2018-20-030

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

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

THE CYBERSECURITY DATA WAREHOUSE NEEDS IMPROVED SECURITY CONTROLS

Highlights

Final Report issued on June 21, 2018

Highlights of Reference Number: 2018-20-030 to the Commissioner of Internal Revenue

IMPACT ON TAXPAYERS

The Cybersecurity Data Warehouse (CSDW) stores taxpayer Personally Identifiable Information. Security weaknesses could adversely affect tax administration and the protection of taxpayer data.

WHY TIGTA DID THE AUDIT

The CSDW was developed for the purpose of collecting security logs from dedicated devices and technology used to protect the IRS network. Following the discovery of a security breach to the Get Transcript application in May 2015, IRS executives decided to transfer transactional audit logs containing taxpayer data from the Get Transcript application to the CSDW. In April 2016, the system began storing taxpayer data to support the newly created Cyber Fraud Analytics and Management team in conducting fraud analysis. The audit was initiated to determine whether the IRS implemented adequate and effective logical and physical access controls over the CSDW.

WHAT TIGTA FOUND

The IRS implemented physical security controls over the CSDW consistent with Federal and agency requirements, encrypted all transmitted data to the CSDW from source systems, and effectively implemented user access, identification, and authentication controls. However, transactional audit logs containing taxpayer data from the Get Transcript application were transferred to the CSDW prior to completing required tasks in the change management process such as updating the system security plan.

In addition, fraud analysts access the transactional audit logs containing taxpayer data to conduct fraud analysis. However, the IRS did not implement CSDW auditing controls that would allow it to monitor fraud analyst and system administrator activities.

Finally, the IRS was unable to provide an inventory of specific systems and applications that transfer taxpayer data to the CSDW until after the completion of audit fieldwork. In our review of the documents, TIGTA found that data are being transferred to the CSDW from key IRS systems such as the Return Review Program and the Customer Account Data Engine 2.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer should ensure that: 1) employees are held accountable for not following established change management policies; 2) all CSDW security documentation including the risk assessment and system security plan are updated and completed as required; 3) automated controls and processes to capture and monitor activities of all IRS personnel with access to taxpayer data in the CSDW are implemented; and 4) a complete and accurate inventory of systems that transfer taxpayer data to the CSDW is maintained.

MANAGEMENT RESPONSE

The IRS agreed with two recommendations and plans to monitor transactions by analysts and administrators and maintain a list of systems that transfer data to the CSDW. The IRS partially agreed with one recommendation and disagreed with another recommendation. We have concerns about the IRS's disagreement with our recommendation. These concerns are discussed in the report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 21, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Cybersecurity Data Warehouse Needs Improved Security Controls (Audit # 201720029)

This report presents the results of our review of security controls over the Cybersecurity Data Warehouse. The overall objective of this review was to determine whether the Internal Revenue Services (IRS) implemented adequate and effective logical and physical access controls over the Cybersecurity Data Warehouse. This audit is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CFAM	Cybersecurity Fraud Analytics and Management
CSDW	Cybersecurity Data Warehouse
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information

Background

The Cybersecurity Data Warehouse (CSDW) was developed to collect and store security logs from dedicated devices used to protect the Internal Revenue Service (IRS) network. This platform allows the IRS to retain log file output data for seven years in accordance with the data retention schedule approved by the National Archives and Records Administration. As of March 2017, the CSDW was a component of the IRS General Support System-1.[1] General Support System-1 provides network infrastructure services to personnel and information systems across the Nation, and serves as the IRS Federal Information Security Modernization Act[2] boundary for monitoring and controlling communications with external networks and information systems.[3] The General Support System-1 protects the IRS network by employing a combination of networking concepts and technologies dedicated to specific functions, such as firewalls, Domain Name System, common communication gateways, and the Computer Security Incident Response Center, which includes intrusion detection systems, security event and information management, Internet proxy systems, and log collection and analysis.

In 2016, the Treasury Inspector General for Tax Administration reported[4] that a security breach involving the Get Transcript application affected 623,401 taxpayers whose tax account information was potentially accessed without authorization.[5] Following this security incident, IRS Cybersecurity organization executives made the decision to transfer taxpayer Personally Identifiable Information (PII) into the CSDW so the newly created Cybersecurity Fraud Analytics and Management (CFAM) team of analysts within the Computer Security Incident Response Center could conduct fraud analysis using this data. The CFAM team consists of 16 fraud analysts who are responsible for monitoring and searching for anomalies in transaction activities and user behavior to identify fraudulent activity based on IRS resource data. The CFAM team uses IRS transactional audit logs containing taxpayer data[6] and specialized tools to run queries to find instances of attempted unauthorized extraction of taxpayer data. The CFAM team is the central fraud analytics function to stop wholesale extraction of PII.

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, and the Enterprise Computing Center in Memphis, Tennessee, during the period June 2017 through

[1] See Appendix IV for a glossary of terms.
[2] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends Chapter 35 of Title 44 of the United States Code to provide for reform to Federal information security.
[3] Title III of the *E-Government Act of 2002*, Pub. L. No. 107-374, 116 Stat. 2899.
[4] Treasury Inspector General for Tax Administration, Ref. No. 2016-40-037, *The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach* (May 2016).
[5] Get Transcript is an online ordering system for individual accounts, not business accounts, available through IRS.gov. The application provides two options: Get Transcript Online and Get Transcript by Mail.
[6] Throughout the remainder of the report, this phrase is often simplified to "taxpayer data."

February 2018. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

User Access Controls and Physical Security Controls Met Federal and Agency Standards

To assess the physical security controls of the CSDW, we visited the Memphis Enterprise Computing Center where the CSDW is located. We performed a walkthrough and observed controls such as the use of guard stations, visitor sign in, metal detectors, Personal Identity Verification card scanners, security cameras, and multiple locked doors to protect and control access to the data center. Those controls were consistent with the minimum security requirements for facilities with a Level IV security classification designation by the Interagency Security Committee.[7] A Level IV facility is defined as any facility with 150,000 square feet or more, more than 450 Federal employees, a high level of public contact and tenant agencies that may include high-risk law enforcement and intelligence agencies, courts, judicial offices, and highly sensitive Government records.[8] The physical security controls we observed were also consistent with National Institute of Standards and Technology (NIST)[9] and Internal Revenue Manual (IRM)[10] minimum physical security requirements.

We reviewed the data transmissions to the CSDW and determined that the IRS encrypts all data transmissions from source systems to the CSDW using one of two techniques. These techniques are Transport Layer Security and Secure File Transfer Protocol administered through the IRS Electronic File Transfer Utility process. These techniques secure and maintain the integrity of data transmissions from source system to the CSDW.

We also reviewed the user access controls for the CSDW and determined that those controls were properly implemented and effective. The IRS established policies and procedures in the IRM to facilitate account management for its information systems.[11] User accounts are granted, modified, and terminated through the Online 5081 process. Our testing confirmed that all CFAM analysts and CSDW system administrators were granted access through the Online 5081 process. We determined that all separated CFAM and CSDW user accounts from

[7] Congressional Research Service, *Federal Building and Facility Security: Frequently Asked Questions* (Mar. 6, 2017).
[8] U.S. Department of Justice, U.S. Marshals Service, *Vulnerability Assessments of Federal Facilities* (June 28, 1995).
[9] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015).
[10] IRM 10.2.14, *Methods of Providing Protection* (Aug. 17, 2016).
[11] IRM 10.8.1, *Information Technology Security - Policy and Guidance; 10.8.1.4.1.1 AC-2 (Account Management)* (July 8, 2015).

March 1, 2017, through September 15, 2017, were disabled, and the last logon date for each account was prior to the user's separation date. Additionally, the IRS utilizes a role-based access control scheme to limit access to data containing PII. Role-based access control restricts information system access and, according to the NIST, simplifies privilege administration for organizations because privileges are not assigned directly to every user but are instead acquired through role assignments.[12] CSDW users are assigned access using two unique role groups. The CFAM analyst group is composed of users who review the transactional audit logs that contain taxpayer data obtained from the CSDW database for fraudulent activities. The CFAM coder group is responsible for parsing the data from the CSDW database to make it readable for the CFAM analysts using a specialized tool. The CFAM coder group does not have readable access to PII.

The IRS implemented effective identification and authentication controls to access taxpayer data in the CSDW. Furthermore, CFAM analysts are required to sign into an additional layer of security to access the CSDW after authenticating to the IRS network using their Personal Identity Verification card and personal identification number to gain access to taxpayer data.

The Security Change Management Process Was Not Properly Followed

The IRS deployed the Get Transcript application in January 2014 and disabled the application on May 21, 2015.[13] Following the security breach, IRS executives made the decision to allow the CSDW to begin receiving Get Transcript application logs that contain taxpayer data. However, the IRS did not follow its Security Change Management process. Specifically, the IRS transferred transactional audit logs containing taxpayer data from the Get Transcript application into the CSDW without completing the change request process as required by Federal and organizational policies and procedures. Furthermore, the IRS did not conduct a risk assessment to consider alternatives or complete key security documentation reflecting this change.

Significant system changes were made to the CSDW without following change request processes or notifying appropriate officials

The NIST requires an organization to review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses. In addition, the NIST requires that configuration change decisions

[12] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *Access Control AC-3 (Access Enforcement).*
[13] The Get Transcript application was re-launched in June 2016.

associated with the information system be documented and retained.[14] The IRM[15] also requires the IRS to ensure that all business and functional unit owners use the Federal Information Security Modernization Act of 2014[16] guidance and standard operating procedures[17] for security configuration management. These procedures require that a security change request must be submitted for changes to existing information systems. The IRS submitted a security change request for review to the Security Change Advisory Board; however, the IRS did not complete the required tasks before it made a significant system change to the CSDW. IRS executives stated that transferring taxpayer data to the CSDW was essential to perform the fraud analysis that could prevent further security incidents involving the Get Transcript application, and therefore did not prioritize system documentation. As a result, the IRS did not follow established security control processes. Two years after the IRS decision to transfer taxpayer data to the CSDW, some controls remain weak and documentation is not complete.

Because the IRS did not follow established change management processes, the General Support System-1 authorizing official was unaware that the CSDW now stores taxpayer data for use in fraud analysis. During our fieldwork, we notified this official that PII is now housed within the CSDW. The IRS introduced new security weaknesses and risk to the CSDW when it began transferring taxpayer data from the Get Transcript application to the CSDW without following the established change management process. For example, if appropriate officials are not aware that PII has been transferred into a system that was not originally designed to protect PII, they cannot adequately protect that data or take steps to prioritize necessary resources to appropriately manage the system from a security and risk perspective.

A risk assessment for the CSDW was not completed or documented

The IRM[18] requires that a risk assessment be conducted and the results documented. Further, the IRM requires that the risk assessment be updated every three years or whenever there are significant changes to the information system or operating environment. The purpose of a risk assessment is to inform decisionmakers and support risk responses by identifying threats, vulnerabilities, potential for exploiting threats, and the likelihood of harm resulting from those threats. The IRS transferred taxpayer data into the CSDW, but did not conduct and document a risk assessment before making this system change.

Without a complete risk assessment document, there is an increased risk that the IRS would be unable to identify relevant threats to the organization. Further, the IRS may be unaware of

[14] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *Configuration Management CM-3 (Configuration Change Control).*
[15] IRM 10.8.1, *Information Technology Security - Policy and Guidance* (July 8, 2015*); CM-3 (Configuration Change Control).*
[16] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends Chapter 35 of Title 44 of the United States Code to provide for reform to Federal information security.
[17] *IRS Security Change Management Standard Operating Procedures*, Version 6.7, (Aug. 20, 2012).
[18] IRM 10.8.1, *Information Technology Security - Policy and Guidance,* RA-3 Risk Assessment (July 8, 2015).

internal and external vulnerabilities that exist that could negatively impact the organization. As part of the overall change management process, the IRS is required to review and update its current security planning policy and procedures every three years or when there is a significant change.

Key security documentation was not updated

When the IRS transferred transactional audit logs containing taxpayer data from the Get Transcript application to the CSDW beginning in April 2016, key security documentation was not updated to reflect this major system change. The IRS Security Change Advisory Board reviewed the change request for transferring taxpayer data to the CSDW and determined that additional tasks required completion prior to the data transfer. The Security Change Advisory Board specified that security artifacts be updated. However, the IRS did not update the CSDW system security plan and privacy impact assessment to reflect the inclusion of taxpayer data as directed by the Security Change Advisory Board.

The NIST requires agencies to update system security plans to address system changes;[19] the IRM also requires the IRS to review the system security plan, at a minimum, annually or as a result of a significant change or problems found during a security controls assessment.[20] We found that the system security plan was not updated to reflect the addition of taxpayer data to the CSDW. The most recent system security plan dated March 31, 2017, states that the CSDW does not contain taxpayer data even though data transfers with PII began in April 2016.

In addition, the IRS did not update the CSDW privacy impact assessment. The NIST requires privacy impact assessments be performed before developing or procuring information systems or initiating programs or projects that collect, use, maintain, or share PII and be updated when changes create new privacy risks.[21] During our fieldwork, the IRS updated its CSDW privacy impact assessment effective September 18, 2017, which now states that the system contains PII including, name, date of birth, and other tax account information.

Without current and complete security documents, the IRS has an increased risk of being unable to identify relevant threats to the organization. Further, the IRS may be unaware of internal and external vulnerabilities that exist which could negatively impact the organization.

[19] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); Planning control PL-2 (System Security Plan).
[20] IRM 10.8.1, *Information Technology Security - Policy and Guidance* PL-2 (*System Security Plan*) (July 8, 2015).
[21] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *Accountability, Audit, and Risk Management* control AR-2 (Privacy Impact and Risk Assessment).

Recommendations

The Chief Information Officer should:

Recommendation 1**:** Ensure that employees are held accountable for not following established change management policies and procedures and completing requirements as quickly as practicable, thus putting PII at risk of exposure to unauthorized access.

> ***Management's Response:*** The IRS disagreed with this recommendation. According to the IRS, this was not an issue of holding employees accountable. In addition, the CSDW was already secured appropriately to protect sensitive data, and the introduction of PII did not require any additional CSDW security controls. The system's security categorization determines which security controls are needed. The security categorization of the CSDW did not change with the introduction of PII and was already at the same level of most IRS systems (including those with PII). Prior to the introduction of PII and through the IRS's continuous monitoring efforts, the CSDW had been assessed and authorized for controls that are sufficient to protect PII. The Security Change Management process documented management controls that needed to be updated, such as updating the systems security package and notification of the authorizing official. While important, these do not affect the security controls applied to the system. The IRS agreed that it can improve its processes and ensure that they are followed, but the IRS stressed that at no time was PII at risk of exposure through the CSDW implementation.
>
> ***Office of Audit Comment:*** IRS employees were aware of the change management process that needed to be completed when PII was added to the CSDW, but they did not compete the required tasks. By not notifying the authorizing official and completing the required tasks, the IRS employees introduced new security weaknesses and risk to the CSDW. With regard to the protection of PII, the IRS does not monitor audit trail data captured from all CFAM analyst and system administrator activities accessing PII. The transfer of PII to the CSDW began in April 2016, and PII remains at risk from internal threats.

Recommendation 2: Ensure that all CSDW security documentation, including but not limited to the risk assessment and system security plans, are updated and completed as required by Federal and agency policies and procedures.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The Cybersecurity organization has completed the applicable CSDW documentation and artifacts including the System Security Plan, Information Security Contingency Plan, and Privacy and Civil Liberties Impact Assessment. However, consistent with IRM 10.8.1, a risk assessment is not required because the CSDW was already secured appropriately to protect sensitive data, and the introduction of PII did not affect any CSDW security controls.

Office of Audit Comment: IRM 10.8.1 control RA-3 (Risk Assessment) requires that the risk assessment be updated every three years or whenever there are significant changes to the information system or operating environment and those results need to be documented. We believe that adding PII to an information system is a significant change in the operating environment that needs to be addressed in a risk assessment. In addition, when the PII was added to the CSDW, the IRS had not implemented complete audit trails and security controls.

Cybersecurity Data Warehouse Audit Trails Were Not Implemented

At the beginning of our audit, the IRS had not implemented complete audit trails and security controls for the CSDW. Because the system now contains PII, the IRS must be able to monitor fraud analysts who have access to taxpayer data, as well as CSDW system administrators, for unauthorized access. According to IRS personnel, they only had the capability to capture basic information such as which user accessed the CSDW and when. Auditing controls were not in place for the CSDW because the system was not originally designed to process and store taxpayer data; therefore, granular auditing controls and capabilities were limited. As of December 2017, the IRS took steps to begin capturing the activities performed by CFAM analysts and CSDW system administrators with access to taxpayer data by deploying a tool that has the capability to record activities in searchable, movie-like audit trails. The tool captures the activities data necessary for user profiling and enables full user session details for forensic investigations. However, the IRS has not established a review process for the tool-generated data, and there is currently no timeline for when monitoring will begin. In addition, although IRS executives stated that the CSDW was the only system available for immediate use at that point in time to process taxpayer data following the Get Transcript application security breach, no formal risk assessment or business case was documented, and other known systems already housing PII with built-in audit trails were not considered.

The IRM[22] requires automated software mechanisms be implemented on information systems that process, store, or transmit taxpayer data to ensure compliance with the Taxpayer Browsing Protection Act.[23] Further, standard operating procedures for audit trails require information technology applications and systems which store or process PII, *e.g.*, taxpayer, personnel, financial data, to capture and record, at a minimum, transactional information and employee and contractor transactions that add, delete, modify, or research a taxpayer's record.[24]

With limited audit trails in place to capture and record CFAM analyst and system administrator activities on the CSDW, the IRS lacks the full capability to monitor or perform periodic reviews

[22] IRM 10.8.1, *Information Technology Security - Policy and Guidance; 10.8.1.4.1.1.8 - Access to Sensitive Information* (July 8, 2015).
[23] 26 U.S.C. §§ 7213, 7213A, and 7431 (2013).
[24] *Enterprise Security Audit Trails, Audit Controls Response, Standard Operating Procedures*, Version 1.0, (July 31, 2017).

of these activities. The IRS is at risk of being unable to identify employees who have violated the Taxpayer Browsing Protection Act and the IRS's unauthorized access policy. Further, the lack of auditing controls hinders IRS management's ability to enforce unauthorized access policies.

Recommendation

Recommendation 3: The Chief Information Officer should ensure that automated controls and processes to capture and monitor the activities of all IRS personnel with access to transactional audit logs containing taxpayer data in the CSDW are implemented.

> ***Management's Response:*** The IRS agreed with this recommendation. During the audit, the Cybersecurity organization implemented enhanced auditing controls for the CSDW to capture the activities performed by analysts and administrators. Efforts are underway to ensure ongoing monitoring of transactions by analysts and administrators.

An Inventory of Systems That Transfer Taxpayer Data to the Cybersecurity Data Warehouse Was Not Maintained

The NIST requires agencies to establish, maintain, and update an inventory that contains a list of all programs and information systems identified as collecting, using, maintaining, or sharing PII.[25] We requested a comprehensive list of all system names that send taxpayer data to the CSDW at the beginning of our fieldwork, but the IRS did not have an inventory of those systems. To address our request, CSDW system administrators were able to provide a comprehensive list of Internet Protocol addresses that are transferring data to the CSDW. The system is divided into two data repositories. The first is the legacy CSDW system that receives system log data from 9,540 unique addresses. These addresses belong to network devices such as firewalls, routers, or switches. The second repository receives transfers from an additional 181 addresses that are associated with IRS systems that contain taxpayer data used by the CFAM team for fraud analysis. We found host names for 179 of the 181 addresses of systems containing PII, but not the specific systems. The CSDW system administrators could not identify the IRS systems comprising the 181 addresses associated with the fraud analysis repository. According to IRS personnel, they did not have the resources to maintain an ongoing list of systems transferring data to the CSDW. We informed IRS executives at the closing conference that we could not obtain this inventory of system names during the audit. The IRS provided a comprehensive list and additional evidence that identified systems that transfer data to the CSDW after the completion of our fieldwork. In our review of the documents, we found

[25] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *Security* control SE-1 (Inventory of Personally Identifiable Information).

that data are being transferred to the CSDW from key IRS systems such as the Return Review Program and the Customer Account Data Engine 2 to help identify potential fraudulent activity.

Recommendation

Recommendation 4**:** The Chief Information Officer should ensure that a complete and accurate inventory of systems that transfer transactional audit logs containing taxpayer data to the CSDW is maintained.

> ***Management's Response*:** The IRS agreed with this recommendation. As noted in the report, after the completion of fieldwork, the IRS provided a comprehensive list and additional evidence that identified systems that transfer data to the CSDW. The IRS will ensure this list is maintained.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS implemented adequate and effective logical and physical access controls over the CSDW. To accomplish our objective, we:

I. Identified all application and data sources contained in the CSDW.

II. Determined the controls and safeguards in place to protect CSDW data.

- A. Obtained and reviewed CSDW documentation such as the system security plan,[1] change requests, and security artifacts and assessed them for accuracy and currency.
- B. Reviewed relevant criteria, policies, and procedures for data storage, *i.e.*, protection of PII and storage and retention requirements.
- C. Interviewed system owners to determine whether they were aware that PII was moved to the CSDW and, if so, determined whether procedures were followed and documented to facilitate the transition, *i.e.*, performing a risk assessment.
- D. Conducted a security controls review that determined what security controls were in place to safeguard CSDW data.
  1. Reviewed controls in place that protect data transmission from the Get Transcript and other applications to the CSDW.
  2. Evaluated whether those controls were adequate to protect CSDW data.

III. Determined whether access controls were implemented for the CSDW.

- A. Reviewed IRS access control policies and procedures for the CSDW.
- B. Interviewed appropriate personnel to gain an understanding of how access to CSDW data are granted, revoked, suspended, and reviewed.
- C. Determined the levels of access and the differences in privileges, *i.e.*, role-based, elevated, privileged.
- D. Evaluated the identification and authentication method in place to access the CSDW.

IV. Determined whether effective physical security controls are in place to protect the CSDW from unauthorized access.

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

A. Determined where the CSDW components are housed and the security level of those facilities, and performed a walk-through.

B. Reviewed the minimum security requirements for protection of CSDW servers and evaluated those servers against that criteria.

C. Evaluated the minimum security control requirements for the computing facility based on the assigned security level and ensured that those controls were in place.

V. Determined whether CSDW activities are monitored and audited.

A. Interviewed appropriate personnel to determine the tools and controls in place for collecting logs and monitoring CSDW activities.

B. Determined the auditable events recorded to logs.

C. Determined whether logs or activities are reviewed periodically and, if so, how frequently. We obtained evidence of those reviews, if available.

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: NIST Special Publication requirements for security controls over Federal information systems; IRM policies related to access control management and system changes; and IRS Information Technology Cybersecurity Security Change Management Standard Operating Procedures. We evaluated these controls by conducting interviews with IRS personnel and reviewing documentation to gain an understanding of policies and procedures related to the IRS's system change management program and safeguards implemented to prevent unauthorized access to taxpayer data.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jena Whitley, Audit Manager
Khafil-Deen Shonekan, Lead Auditor
Nicholas Reyes, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Computer Security Incident Response Center	Is responsible for preventing, detecting, and responding to computer security incidents targeting the IRS's enterprise information technology assets. It also provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS.
Customer Account Data Engine 2	A major component of the IRS's Modernization Program. The system consists of current and planned databases and related applications that work with the IRS Master File system. Version 2 was created to address risks identified in its predecessor (Customer Account Data Engine) and to implement fundamental changes to the core IRS business systems.
Electronic File Transfer Utility	A tool that moves data in a controlled, structured, and secured environment through the organization.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
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.
Internet Protocol Address	The unique numbers assigned to every computer or device that is connected to the Internet.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal agency operations and assets.

Term	Definition
Online 5081 Application	A web-based application that provides automated submission, approval, re-certification, and filing of a Form 5081, *Information System User Registration/Change Request*, for access to information systems and applications on a Service-wide basis.
Personal Identification Number	A password consisting only of decimal digits.
Personal Identity Verification Card	Physical artifact, *e.g.*, identity card, "smart" card, issued to an individual that contains stored identity credentials, *e.g.*, photograph, cryptographic keys, digitized fingerprint representation, such that the claimed identity of the cardholder may be verified against the stored credentials by another person or an automated process.
Privacy Impact Assessment	An analysis of how information is handled: 1) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Return Review Program	A system used to review individual refund tax returns. It also provides limited support for business returns and balance due returns claiming the Earned Income Tax Credit.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation arising through the operation of an information system.
Secure File Transfer Protocol	A secure version of File Transfer Protocol, which facilitates data access and data transfer over a Secure Shell data stream. It is part of the Secure Shell Protocol.
Security Change Advisory Board	Meets weekly to review all IRS security change requests and collaborates to determine the Federal Information Security Management Act Inventory Level of a system. During these meetings, the current status of each security change request is reviewed and updated, with next steps determined and any open issues discussed.

Term	Definition
System Log	System or device-related entries consisting of the message type and severity, a timestamp, the hostname or Internet Protocol address of the source of the log, and log content.
System Security Plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Transport Layer Security	An authentication and security protocol widely implemented in browsers and Web servers.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

May 08, 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – The Cybersecurity Data Warehouse Needs Improved Security Controls (Audit # 201720029) (e-trak # 2018-01770)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss report observations. We appreciate that your report acknowledged that the Cybersecurity Data Warehouse (CSDW) met Federal and Agency Standards for user access and physical security controls were properly implemented.

The IRS is committed to the protection of all data including the taxpayer transaction Personal Identifiable information (PII). CSDW was already secured appropriately to protect sensitive data and the introduction of PII did not require any additional CSDW security controls. The system's security categorization determines which security controls are needed. The security categorization of CSDW did not change with the introduction of PII and was already at the same level of most IRS systems (including those with PII). Prior to the introduction of the PII and through the IRS's continuous monitoring efforts, CSDW had been assessed and authorized for controls that are sufficient to protect PII. We agree we can improve our processes and ensure they are followed, but we must stress that at no time was PII at risk of exposure through the CSDW implementation.

The attached is our detailed planned corrective actions to implement the audit report's recommendations. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment

Attachment

Draft Audit Report Cybersecurity Data Warehouse (Audit # 201720029)

RECOMMENDATION #1: The Chief Information Officer should ensure that employees are held accountable for not following established change management policies and procedures and completing requirements as quickly as practicable, thus putting PII at risk of exposure to unauthorized access.

CORRECTIVE ACTION #1: We disagree with the recommendation. This was not an issue of holding employees accountable. In addition, the CSDW was already secured appropriately to protect sensitive data and the introduction of PII did not require any additional CSDW security controls. The system's security categorization determines which security controls are needed. The security categorization of CSDW did not change with the introduction of PII and was already at the same level of most IRS systems (including those with PII). Prior to the introduction of the PII and through the IRS's continuous monitoring efforts, CSDW had been assessed and authorized for controls that are sufficient to protect PII. The Security Change Management process documented management controls that needed to be updated such as updating the systems security package and notification of the AO. While important, these do not impact the security controls applied of the system. We agree we can improve our processes and ensure they are followed, but we must stress that at no time was PII at risk of exposure through the CSDW implementation.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should ensure that all CSDW security documentation, including but not limited to the risk assessment and system security plans, are updated and completed as required by Federal and agency policies and procedures.

CORRECTIVE ACTION #2: We partially agree with this recommendation. Cybersecurity has completed the applicable Cybersecurity Data Warehouse (CSDW) documentation and artifacts including the System Security Plan (SSP), Information Security Contingency Plan (ISCP), and the Privacy and Civil Liberties Impact Assessment (PCLIA). However, consistent with Internal Revenue Manual (IRM) 10.8.1, a risk assessment is not required since CSDW was already secured appropriately to protect sensitive data and the introduction of PII did not impact any CSDW security controls.

Attachment

Draft Audit Report Cybersecurity Data Warehouse (Audit # 201720029)

IMPLEMENTATION DATE: February 16, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Chief Information Officer should ensure that automated controls and processes to capture and monitor the activities of all IRS personnel with access to transactional audit logs containing taxpayer data in the CSDW are implemented.

CORRECTIVE ACTION #3: We agree with this recommendation. During the audit, Cybersecurity implemented enhanced auditing controls for Cybersecurity Data Warehouse (CSDW) to capture the activities performed by analysts and administrators. Efforts are underway to ensure ongoing monitoring of transactions by analysts and administrators.

IMPLEMENTATION DATE: January 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Information Officer should ensure that a complete and accurate inventory of systems that transfer transactional audit logs containing taxpayer data to the CSDW is maintained.

CORRECTIVE ACTION #4: We agree with this recommendation. As noted in the report after the completion of field work, the IRS provided a comprehensive list and additional evidence that identified systems that transfer data to the CSDW. The IRS will ensure this list is maintained.

IMPLEMENTATION DATE: February 20, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report Cybersecurity Data Warehouse (Audit # 201720029)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.