TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened

September 21, 2022

Report Number: 2022-20-051

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

HIGHLIGHTS: Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened

Final Audit Report issued on September 21, 2022 **Report Number 2022-20-051**

Why TIGTA Did This Audit

In an effort to improve customer service and the taxpayer experience, the IRS launched the Taxpayer Digital Communications (TDC) platform. The platform enables faster communication as well as offers taxpayers and their authorized representatives the ability to securely send and receive electronic messages and documents to and from IRS agents and customer service representatives.

This audit was initiated to assess the security and access controls over the TDC platform.

Impact on Tax Administration

Without effective security and access controls, the TDC platform is susceptible to data loss and manipulation as well as unauthorized access and disclosure of taxpayer data. In addition, the TDC platform is vulnerable to human errors or actions committed with malicious intent. People acting with malicious intent can use their accesses to obtain sensitive information, commit fraud and identity theft, disrupt operations, and launch attacks against the IRS.

What TIGTA Found

The eGain Corporation is the dedicated managed service provider (MSP) for the TDC platform. The TDC platform, including its 12 installations in production, are stored on the eGain platform in a Federal Risk and Authorization Management Program authorized Amazon Web Services GovCloud. Production servers on which the TDC platform resides are encrypted to protect TDC installation data, and configuration settings for password length and complexity are in compliance with Federal and local requirements.

However, Federal Risk and Authorization Management Program security reviews for continuous monitoring are not being conducted by the IRS to ensure that the Amazon Web Services GovCloud's security posture remains sufficient for the TDC platform. Two critical and three high severity rated antivirus software releases were not installed on the TDC platform, and it was using an outdated version of the antivirus software for approximately one year.

TIGTA reviewed 175 security vulnerabilities and determined that the eGain MSP did not timely remediate four (2.3 percent) critical security vulnerabilities. The remediation time ranged from 16 to 42 calendar days. In addition, audit trails are not being reviewed.

The TDC platform has 3,939 distinct total users; however, 681 users were not authorized to have access to the TDC platform, and 498 users were authorized but did not have access to the TDC platform. Of the 3,258 authorized users, 735 users were not timely recertified. Finally, 1,237 user accounts were not timely disabled, quarantined, or removed due to inactivity, of which 646 user accounts were never logged in.

What TIGTA Recommended

TIGTA made 11 recommendations to the Chief Information Officer. They include ensuring that the standard operating procedures are updated to require continuous monitoring security reviews and the security reviews are conducted; eGain MSP personnel timely upgrade antivirus software in accordance with requirements; users are both authorized and have access to the TDC platform; and a process is developed to timely identify, quarantine, and remove user accounts for inactivity in accordance with requirements.

The IRS agreed with all 11 recommendations. The IRS plans to update the standard operating procedures to require continuous monitoring security reviews; conduct Annual Security Control Assessments; and conduct reviews to ensure that users are both authorized and have access to the TDC platform. In addition, the IRS stated that it now requires the eGain MSP to provide weekly patching and antivirus definition updates, including timeliness reporting and that the IRS and eGain MSP have changed the inactivity parameter to ensure that personnel timely disable, quarantine, and remove user accounts in accordance with requirements.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 21, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened (Audit # 202220014)

This report presents the results of our review to assess the security and access controls of the Taxpayer Digital Communications platform. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] Resources*.

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

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

Background

In an effort to improve customer service and the taxpayer experience, the Internal Revenue Service (IRS) launched the Taxpayer Digital Communications (TDC) Secure File Sharing – Secure Messaging platform (hereafter referred to as the TDC platform). Within the Information Technology organization, the User and Network Services function's Contact Center Support division provides oversight of the TDC platform. The Contact Center Support division's mission is "to provide the technology to make customer contact happen." The TDC platform enables faster communication as well as offers taxpayers and their authorized representatives the ability to securely send and receive electronic messages and documents to and from IRS agents and customer service representatives.[1]

The TDC platform uses the eGain Solve software,[2] which is developed and maintained by the eGain Corporation. The eGain Corporation is also the dedicated managed service provider (hereafter referred to as the eGain MSP) for the TDC platform. The TDC platform includes various installations that have been created to meet IRS business operating division requirements. As of June 27, 2022, 12 approved TDC installations are in production[3] and two are in development.[4] The TDC platform, including the installations, are stored on the eGain platform in an Amazon Web Services (AWS) GovCloud, which is Federal Risk and Authorization Management Program (FedRAMP) authorized. FedRAMP is a U.S. Federal Governmentwide program that provides a standardized approach to security assessments, authorizations, and continuous monitoring for cloud products and services. According to the *Taxpayer Digital Communications Overview*,[5] the eGain platform provides a wide range of capabilities that directly support the Taxpayer First Act of 2019,[6] including:

- Secure Messaging – Taxpayers can quickly and securely communicate and share documents with agents.
- Text Chat – Real-time chat assistance allows for both unauthenticated and authenticated text chats. Customer service representatives can manage multiple text chats at once. Over 50 percent of text chat sessions include chat deflection by providing taxpayers with automated information to assist them without escalating to a live chat. The IRS currently offers English and Spanish text chats; however, the eGain platform supports all of the IRS's top 20 languages. Authenticated users can also attach documents.
- Superchat – Enables customer service representatives to proactively engage taxpayers beyond text chat with video, voice, and co-browse capabilities.

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

[2] A commercial off-the-shelf product that is a cloud-based customer engagement hub.

[3] The 12 TDC installations in production include the: 1) Advanced Pricing and Mutual Agreement; 2) Affordable Care Act Branded Prescription Drug Feepayers; 3) Appeals Officer; 4) Automated Collection System Chat; 5) Automated Underreporter; 6) Centralized Authorization File Units Intake; 7) Collection Chatbot; 8) Compliance; 9) Correspondence Exam; 10) Refund Status Chatbot; 11) Secure Access; and 12) Tax Exempt and Government Entities-Wide.

[4] The two TDC installations in development are the Appeals Chatbot and Opportunity Zone.

[5] Dated April 26, 2021.

[6] Pub. L. No. 116-25.

- Virtual Assistant – Provides answers and help 24 hours a day, 7 days a week, without requiring a customer service representative.
- Click to Call – Taxpayers can click a link to speak directly with a customer service representative from within a secure portal. With full integration, customer service representatives will have access to the information from chat and virtual assistant activity, providing context at the beginning of the conversation.

TDC installations are managed independently by their respective business operating division and vary on how taxpayers are authenticated. Six TDC installations use the Secure Access Digital Identity system, and three TDC installations use a manual method to authenticate taxpayers. Secure Access Digital Identity authenticates taxpayers by using a credential service provider to verify the identity of the taxpayer. Manual authentication is used because the Secure Access Digital Identity does not currently have the capability to systemically authenticate representatives of companies, local Governments, *etc*. Instead, manual authentication is attained by obtaining a signed consent form and establishing a memorandum of understanding between the IRS and a representative of the company or local Government. It also requires a one-time passcode be sent to the representative's verified e-mail address that must be entered prior to accessing the TDC installation. The remaining three TDC installations provide only general guidance to taxpayers on how to complete the authentication process, make payment, and obtain refund status, and do not require authentication.

Results of Review

The IRS has taken some steps to protect TDC installation data stored on the eGain platform. Our review found that all 43 eGain platform production servers on which the TDC platform resides are encrypted and in compliance with the Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*.[7] Encryption was first enabled on July 11, 2016, which was prior to the launch of the first TDC installation on December 10, 2016. In addition, our review found that the TDC platform configuration settings for password length and complexity (*i.e.*, use of uppercase and lowercase letters, numbers, and special characters) are in compliance with Internal Revenue Manual (IRM) 10.8.24, *Information Technology (IT) Security – Cloud Computing Security Policy*.[8] However, we also found that security and access controls over the TDC platform should be improved. In addition, the Treasury Inspector General for Tax Administration is concurrently performing a related audit on the TDC program.[9]

Security Controls Should Be Improved

The Information Technology organization's Cybersecurity function ensures compliance with Federal statutory, legislative, and regulatory requirements to assure the confidentiality, integrity,

[7] Dated May 25, 2001.

[8] Dated September 28, 2021.

[9] Treasury Inspector General for Tax Administration, Report No. 2022-30-068, *More Should Be Done to Expand and Increase Use and Availability of the IRS's Taxpayer Digital Communication Tools* (Sept. 2022).

and availability of electronic systems, services, and data, including the TDC platform. Without effective security controls, the TDC platform is vulnerable to human errors or actions committed with malicious intent. People acting with malicious intent can use their accesses to obtain sensitive information, commit fraud and identity theft, disrupt operations, and launch attacks against the IRS.

We found that security controls over the TDC platform need improvement, specifically in the areas of FedRAMP security reviews for continuous monitoring, virus protection, vulnerability remediation, and audit trail reviews.

FedRAMP security reviews for continuous monitoring are not being conducted

The IRS is not conducting required FedRAMP security reviews for continuous monitoring to ensure that the AWS GovCloud's security posture remains sufficient for the TDC platform. According to both the General Services Administration's *FedRAMP Security Assessment Framework* [10] and *FedRAMP Continuous Monitoring Strategy Guide*,[11] the continuous monitoring phase of the FedRAMP authorization process is critical to ensuring that the cloud service provider's (CSP) security posture continues to meet Federal cloud service requirements. The framework and guide provide guidance on continuous monitoring as well as a schedule of activities and artifacts required by the CSP and a third-party assessment organization. The CSP must monitor its security controls, assess them on a regular basis, and demonstrate that the security posture of its service is continuously acceptable. The third-party assessment organization is responsible for independently verifying and validating the controls implemented and the test results for the CSP. Specifically, the third-party assessment organization is responsible, in part, for:

- Assessing controls on an ad hoc basis as requested by an agency's authorizing official for any changes made to the system by the CSP.
- Performing penetration testing at least annually.
- Performing annual vulnerability scans of operating systems, web applications, and databases.
- Submitting a security risk assessment report to the agency's authorizing official one year after the CSP's authorization date and each year thereafter.

In addition, the guide requires that the CSP and third-party assessment organization provide evidentiary information to the agency's authorizing official at least monthly (*e.g.*, vulnerabilities mitigation report), annually (*e.g.*, penetration testing report), every three years (*e.g.*, updated security risk assessment report), and on an as-needed basis after a FedRAMP authorization is granted. In turn, the agency's authorizing official is required to oversee the CSP's continuous monitoring activities for any significant changes and review all security artifacts provided by the CSP, third-party assessment organization, or FedRAMP to ensure that the CSP's security posture remains sufficient for their agency's use of the system. The agency's authorizing official should use this information to make risk-based decisions of the ongoing authorization of the system for their agency.

[10] Dated November 15, 2017.

[11] Dated April 4, 2018.

Although the AWS GovCloud was FedRAMP-authorized on June 21, 2016, the Cybersecurity function's Security Risk Management organization management stated that they have not conducted FedRAMP security reviews for continuous monitoring of the AWS GovCloud for the TDC platform.[12] Management added that they have not conducted these reviews because the Federal Information Security Modernization Act Processes and Controls Management Cloud team was not operational until July 2019 and that the CSP continuous monitoring standard operating procedures were not developed to provide guidance. On January 8, 2020, the team developed and released the *IRS Cloud Continuous Monitoring Strategy Standard Operating Procedures*, which provides security review responsibilities, activities, and deliverables for continuous monitoring. We reviewed the standard operating procedures and found that there is no clear timeline for the IRS to begin its FedRAMP security reviews for continuous monitoring of CSPs. Without guidance clearly stating when FedRAMP security reviews for continuous monitoring should begin, Security Risk Management organization personnel may be unaware that continuously monitoring the security postures of CSPs should begin at the time FedRAMP authorizations are granted.

In addition, Security Risk Management organization management stated that the Cybersecurity function conducted FedRAMP security reviews more recently of other IRS systems being deployed into the AWS GovCloud, giving them a "view into (the) AWS GovCloud's security posture." However, these reviews occurred during Calendar Years 2020 and 2021, which is approximately four years after the AWS GovCloud's FedRAMP was authorized and the initial security review was conducted on September 30, 2016, to obtain an authorization to operate for the TDC platform. Security Risk Management organization management further stated that *"...the Federal Information Security Modernization Act Processes and Controls Management Cloud team will be following up with these legacy cloud systems to review the appropriate FedRAMP packages as outlined in the standard operating procedures by the end of the Federal Information Security Modernization Act Year (June 30, 2022)."*

The Chief Information Officer should ensure that:

Recommendation 1: *IRS Cloud Continuous Monitoring Strategy Standard Operating Procedures* is updated requiring that security reviews for continuous monitoring begin when the CSP is first FedRAMP authorized.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will update the *IRS Cloud Continuous Monitoring Strategy Standard Operating Procedures* to require that continuous monitoring begins when a CSP is first FedRAMP authorized.

Recommendation 2: FedRAMP security reviews for continuous monitoring are conducted to ensure that the AWS GovCloud's security posture remains sufficient for the TDC platform.

> **Management's Response:** The IRS agreed with this recommendation. The Annual Security Control Assessment for eGain (TDC commercial implementation) was completed on May 4, 2022, and will be conducted each year hence forth. This action ensures that

[12] The IRS initially procured the eGain platform as a private MSP for the TDC platform, and it was not required to be FedRAMP authorized. On May 31, 2021, the eGain Corporation became the Software-as-a-Service solution and was then required to be FedRAMP authorized. On December 15, 2021, the eGain platform was FedRAMP authorized.

the AWS GovCloud's security posture remained sufficient as part of the FedRAMP security review for continuous monitoring.

The eGain platform was not running the latest version of antivirus software

Updated antivirus software is periodically released by the vendor to provide fixes to known security issues and includes cumulative fixes from previous updates. The releases may also include new or enhanced features as well as remove outdated features to improve the stability of the software. In addition, a severity rating (*e.g.*, critical, high, medium, low) is assigned for each antivirus software release that defines the urgency for installing the release.

We obtained screenshots of the eGain MSP's dashboard to identify the version of the antivirus software running on the eGain platform and conducted research on the antivirus software vendor website to identify the most current version of the antivirus software available. Our comparison of the antivirus software versions determined that eGain MSP personnel did not install two critical and three high severity rated antivirus software releases and were using an outdated version of the antivirus software for approximately one year. This potentially affected the 43 production servers on which the TDC platform resides. Figure 1 provides the antivirus software releases since the eGain MSP last updated its antivirus software from February 2021 through February 2022, its severity rating, whether it was installed, and examples of security fixes that were not applied.

Figure 1: Analysis of Antivirus Software Releases

Antivirus Software Release Date	Antivirus Software Severity Rating	Antivirus Software Installed?	Examples of Security Fixes That Were Not Applied With the Antivirus Software Releases
February 2021	Critical	Yes	Not Applicable
April 2021	High	No	On-Access scans[13] took extra time to detect ransomware.
June 2021	High	No	ePolicy Orchestrator[14] cloud customers were unable to see an Exploit Prevention Signature[15] in their policy.
September 2021	Critical	No	Unspecified error caused files to be skipped during an On-Demand scan.[16]
November 2021	Critical	No	On-Access scan did not start successfully.
February 2022	High	No	Not Applicable

Source: Endpoint Security 10.7x – Release Notes – Windows, dated February 2022.

According to IRM 10.8.1, *Information Technology (IT) Security – Policy and Guidance*,[17] antivirus software must be installed and updated as new releases are available. In addition, IRM 2.17.1,

[13] It examines files as the user accesses them, providing continuous, real-time detection of threats.

[14] It is the central software repository for all antivirus software vendor product installations, updates, and other content.

[15] It detects for encrypted credential thefts.

[16] It scans files, folders, memory, and the registry for any malware that could infect a computer. It can be configured for when and how often the scans occur and can scan systems manually, at a scheduled time, or at startup.

[17] Dated September 28, 2021.

Infrastructure Currency, Infrastructure Currency Policy for Software,[18] states that commercial off-the-shelf products, such as the eGain platform, shall run the most current software version or the immediately preceding version approved in the IRS's Enterprise Standards Profile.[19] Further, the antivirus software vendor recommends that clients always upgrade to the most current release of its antivirus software to be protected from the latest threats and that failure to apply the upgrade might result in a severe business impact.

The eGain MSP did not update the antivirus software because its personnel were unaware of the IRM requirements. The eGain MSP Senior Project Manager explained that they configure the eGain platform to automatically install security update files on a daily basis, but only update the antivirus software on an as-needed basis when an update addresses a security issue with the eGain software or if the update fixes something that is relevant to the environment. However, we believe that antivirus software with a critical or high severity rating should be relevant to the environment and timely upgraded.

Management Action: We notified the Senior Project Manager of the IRM requirement and the antivirus software vendor's recommendation. On March 15, 2022, eGain MSP personnel upgraded the eGain platform with the latest antivirus software version. The Senior Project Manager stated that they upgraded the software due to the vendor's recommendation and the IRS's requirements.

Recommendation 3: The Chief Information Officer should ensure that adequate oversight is provided to ensure that eGain MSP personnel timely upgrade antivirus software in accordance with IRM requirements.

Management's Response: The IRS agreed with this recommendation. The IRS now requires that the eGain MSP provide weekly patching and antivirus definition updates to include timeliness reporting. The eGain MSP provides a monthly summary of the patching and antivirus definition updates report in the monthly report to the IRS. The *IRS System Security Plan for Taxpayer Digital Communications*[20] will be updated to reflect this requirement.

Not all critical security vulnerabilities were timely remediated

The eGain MSP uses a scanning tool to identify security vulnerabilities on the eGain platform. Identified vulnerabilities are tracked with a software tool that captures when a ticket is created and resolved, among other information. We requested and received a report that identified all security vulnerabilities discovered from July 2016 through February 4, 2022, to determine whether they were timely remediated. However, the tracking tool does not capture the date the security vulnerability was discovered. According to the eGain MSP Senior Project Manager, the issue ticket creation date is the same date as when the security vulnerability was discovered. To verify, we judgmentally[21] selected 11 security vulnerabilities from the issue tracking report as well as requested and received their respective vulnerability scans. We found that the vulnerability scan discovery date matched the issue ticket creation date for 10 of the 11 security

[18] Dated October 26, 2020.

[19] The central repository for IRS-approved information technology products and standards.

[20] Dated July 26, 2021.

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

vulnerabilities selected for review. For the remaining security vulnerability, the issue ticket was created one day after the vulnerability was discovered. Given the results of our judgmental sample, we believe that the ticket creation date captured was a fair indication of when the security vulnerability was discovered.

The eGain MSP documented 177 security vulnerabilities in its issue tracking report. Of the 177 security vulnerabilities, 162 included a severity rating – 9 critical, 52 high, 74 medium, and 27 low. The eGain MSP did not provide a severity rating for the remaining 15 security vulnerabilities. However, 13 of the 15 security vulnerabilities were remediated in less than 15 calendar days, which met the minimum required remediation time frame for critical vulnerabilities. As a result, we included them in our population for review, giving the eGain MSP credit for timely remediating the 13 security vulnerabilities. In total, we reviewed 175 security vulnerabilities and determined that the eGain MSP did not timely remediate four (2.3 percent) critical security vulnerabilities. The remediation time ranged from 16 to 42 calendar days, averaging 24 calendar days. All four critical security vulnerabilities are related to security updates for Microsoft servers.

According to IRM 10.8.50, *Information Technology Security, Servicewide Security Patch Management*,[22] all security vulnerabilities shall be assigned either a critical, high, medium, or low severity rating and be remediated within 15, 30, 120, or 180 calendar days, respectively, for Internet-accessible systems. Remediation begins when a security vulnerability is discovered.

We found that the *IRS System Security Plan for Taxpayer Digital Communications* did not identify the TDC platform as an Internet-accessible system and incorrectly stated that critical security vulnerabilities be remediated within 30 calendar days, rather than within 15 calendar days as required. As a result, the eGain MSP Senior Project Manager stated that they had applied the wrong time frame for remediating the critical security vulnerabilities. In addition, the manager stated that they delayed the installation of a patch due to potential authentication failures on printer servers.

The Chief Information Officer should ensure that:

Recommendation 4: Management oversight is provided to ensure that the eGain MSP timely remediates identified security vulnerabilities in accordance with the remediation time frames for Internet-accessible systems.

> **Management's Response:** The IRS agreed with this recommendation. The IRS has implemented this recommendation and receives a weekly report from the eGain MSP that verifies all patching and security vulnerabilities are being addressed. The *IRS System Security Plan for Taxpayer Digital Communications* will be updated to reflect the new requirement.

Recommendation 5: The *IRS System Security Plan for Taxpayer Digital Communications* is updated to reflect the correct vulnerability remediation time frame and that the TDC platform is an Internet-accessible system.

> **Management's Response:** The IRS agreed with this recommendation. The patching process has been implemented, and the scanning schedule now occurs weekly. The *IRS*

[22] Dated November 25, 2020.

System Security Plan for Taxpayer Digital Communications will be updated to reflect that the platform is an Internet-accessible system.

Audit trails are not being reviewed

IRM 10.8.1 and the *IRS System Security Plan for Taxpayer Digital Communications* require audit trails to be reviewed two to three times a week. In addition, Internal Revenue Code § 6103 and the Taxpayer Browsing Protection Act of 1997[23] require the IRS to detect and monitor unauthorized access and disclosure of taxpayer records.

In March 2022, the Cybersecurity function's Counter Insider Threat Operations branch management stated that audit trail reviews are not being conducted because their personnel's roles and permissions were not properly set up in Splunk by the Cybersecurity function's Architecture and Implementation group. Splunk is a security information and event management tool used for real-time security analytics, detecting targeted attacks and data breaches, and forensic analysis of log (audit trail) data. Counter Insider Threat Operations branch management also stated that they did not perform audit trail reviews because there was a data integrity issue with the audit records in Splunk. The audit records did not contain Taxpayer Identification Numbers, which caused the records to be inaccurate.

We inquired with Architecture and Implementation group personnel about the roles and permissions not being properly set up. They provided screenshots from Splunk that showed the roles and permissions were set up for Counter Insider Threat Operations personnel. In September 2020, the Counter Insider Threat Operations branch was notified that audit trails were implemented and that they should begin their audit trail reviews.

In addition, when Counter Insider Threat Operations branch management informed us of the data integrity issue with the audit records, we obtained and reviewed the *TDC Audit Worksheet*.[24] The worksheet identifies the type of data an audit record should contain. A review of the document determined that only certain audit records contain Taxpayer Identification Numbers, explaining why some of the audit records did not contain them.

Recommendation 6: The Chief Information Officer should ensure that the Counter Insider Threat Operations branch starts reviewing the audit trails for the TDC platform.

Management's Response: The IRS agreed with this recommendation. The Annual Security Control Assessment for eGain (TDC commercial implementation) was completed on May 4, 2022, and identified that the audit trail capture was not functioning as required. The IRS remediated the issue, and the audit log capture resumed prior to the end of May 2022. The Counter Insider Threat Operations branch will continuously monitor eGain audit trails per IRM guidelines.

Access Controls Should Be Improved

Without effective access controls, the TDC platform is susceptible to data loss and manipulation as well as unauthorized access and disclosure of taxpayer data. We found that access controls

[23] 26 U.S.C. §§ 7213, 7213A, and 7431 (2018).

[24] Dated September 23, 2020.

over the TDC platform need improvement, specifically in the areas of account management and password policy enforcement.

Not all users were authorized to access the TDC platform

When a user needs access to a system, the user requests access and specifies their user role (*i.e.*, privileged, nonprivileged) through the Business Entitlement Access Request System (BEARS).[25] The user's manager and the system administrator approve the request in the BEARS. Once approved, the system administrator creates a user account and assigns the appropriate user role. The process is the same when requesting to remove a user from a system, but the action can be initiated by either the user or manager.

We obtained user account data from the BEARS, a listing of 3,258 users with authorizations to the TDC platform as of January 6, 2022, and from the eGain MSP, a listing of 3,441 users having access to the TDC platform as of February 4, 2022. Our review and comparison of the two listings determined that, of 3,939 distinct total users:

- 2,760 (70.1 percent) users were authorized in the BEARS and have access to the TDC platform.
- 498 (12.6 percent) users were authorized in the BEARS and did not have access to the TDC platform.
- 681 (17.3 percent) users with access to the TDC platform were not authorized in the BEARS.

In total, we identified 1,179 incorrect or missing authorizations. Figure 2 provides a summary of our analysis.

Figure 2: Analysis of TDC Platform User Accounts

Account Type	Users With Authorizations in the BEARS Who Have Access to the TDC Platform	Users With Authorizations in the BEARS Who Do Not Have Access to the TDC Platform	Users With No Authorizations in the BEARS Who Have Access to the TDC Platform	Total Users
Privileged	3[26]	4	12	19
Nonprivileged	2,757	494	669	3,920
Totals	2,760	498	681	3,939

Source: Treasury Inspector General for Tax Administration's analysis of user account data from the BEARS and the eGain MSP of TDC platform users, dated January 6, and February 4, 2022, respectively.

We also found that, while only seven [4 + 3] users have authorizations in the BEARS for privileged access, 70 users had privileged access on the TDC platform. Of the 70 users, 57 users

[25] The BEARS is replacing the Online 5081 system. The Online 5081 system is a web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.

[26] Two of the three users with authorizations in the BEARS for privileged access did not have privileged access on the TDC platform.

have authorizations, but not for privileged access; 12 users have no authorizations at all; and only one user has an authorization and access for privileged access. Six of the seven users with authorizations in the BEARS for privileged access did not have privileged access on the TDC platform.

In addition, we found users who have a continued business need for access are not timely recertified. Specifically, we determined that 735 (22.6 percent) of the 3,258 [498 + 2,760] users with authorizations in the BEARS were not timely recertified. Three of the 735 users not timely recertified have privileged access to the TDC platform; the remaining 732 users have nonprivileged access. The delays ranged from 24 to 119 calendar days for privileged users, averaging 67 calendar days, and from 1 to 178 calendar days for nonprivileged users, averaging 33 calendar days.

During our review, the IRS was in the process of replacing the Online 5081 system with the BEARS. The Continuous Diagnostics and Mitigation team migrated all user account data, except the employee and manager recertification dates, for the TDC platform from the Online 5081 system to the BEARS by December 10, 2021.[27] IRS management made a business decision to not recertify users' accesses for systems in which their user account data were already migrated to the BEARS. Rather, the IRS initiated a "manager recertification campaign" that began on May 16, 2022, and is scheduled to end on June 30, 2022, requiring managers to recertify all their employees' system accesses during this time frame. Moving forward, the "manager recertification campaign" will require managers to recertify all privileged users semiannually and all nonprivileged users annually during specified times of the year.

IRM 10.8.1 requires that the Service-wide process, the BEARS, be used to register all users requiring access to any IRS information technology resource. It also requires that the principle of least privilege be employed, allowing authorized accesses only for users for whom it is necessary to accomplish assigned tasks in accordance with IRS missions and business functions. In addition, the IRM requires that privileged and nonprivileged accounts be reviewed for compliance with account management requirements (*e.g.*, recertify that there is a continued business need), semiannually and annually, respectively.

Given that 681 users were identified with access to the TDC platform without authorizations in the BEARS and that 498 users were identified with authorizations in the BEARS but no access to the TDC platform, we believe and Contact Center Support division management agrees that the migration of user account data from the Online 5081 system to the BEARS contributed to this finding. However, we also believe that the system administrators did not perform their duties as required to create a user account or grant privileged access only when authorized through the BEARS.

After we discussed these items with the IRS, the Federal Information Security Modernization Act Processes and Controls Management Cloud team conducted a Cloud-Security Assessment and Authorization assessment. We reviewed the assessment documentation in which the IRS determined that the TDC platform system administrators are now following established procedures in accordance with IRM requirements for adding and removing users as well as granting privileged user role access.

[27] With the BEARS, employees are no longer required to self-recertify; instead, managers are required to recertify for their employees that there is a continued business need for system access.

Management Action: On March 28, 2022, the Cybersecurity function opened a Plan of Action and Milestones with a planned completion date of December 31, 2022, to resolve the BEARS recertification issue.

Recommendation 7: The Chief Information Officer should reconcile between users having authorizations in the BEARS and users having access to the TDC platform and resolve any discrepancies identified by adding or removing the authorization or user account based upon whether there is a business need for access.

Management's Response: The IRS agreed with this recommendation. The IRS will review BEARS entitlements access to ensure that they align with eGain systems access and address discrepancies for user entitlement authorizations. The business units will be required to provide quarterly account reconciliation reports, and the Information Technology organization will review the quarterly BEARS reports to reconcile with eGain reports for continuity.

Inactive user accounts remained active on the TDC platform

Using the same eGain MSP listing of 3,441 users having access to the TDC platform, we determined that 1,237 (35.7 percent) of the 3,465 user accounts,[28] of which 20 user accounts have privileged access, should have been disabled, quarantined,[29] or removed due to inactivity. The time frame for inactivity ranged from 78 to 2,057 calendar days, averaging 335 calendar days. Two of the privileged user accounts that should have been quarantined both had the ability to make modifications to the system's configurations, manage application security, and add and remove users. We also determined that 646 (52.2 percent) of the 1,237 user accounts were never logged in. Figure 3 presents the result of our analysis.

Figure 3: Analysis of User Accounts for Inactivity

Account Type	User Accounts That Should Be Disabled	User Accounts That Should Be Quarantined	User Accounts That Should Be Removed	Total User Accounts
Privileged	1	16	3	20
Nonprivileged	339	524	354	1,217
Totals	340	540	357	1,237

Source: Treasury Inspector General for Tax Administration's analysis of the eGain MSP listing of user accounts on the TDC platform as of February 4, 2022.

Further analysis of the user account data against the Treasury Integrated Management Information System[30] determined that three accounts belonged to employees who had left the IRS. Two of the user accounts were last logged in 217 and 246 calendar days ago. The third user account was created 345 calendar days ago and was never logged in.

[28] Ten users had an additional 24 user accounts for different TDC installations and user roles.

[29] Quarantined accounts are disabled accounts whose user rights and permissions have been revoked.

[30] The official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. It is outsourced to the U.S. Department of Agriculture's National Finance Center and managed by the Department of the Treasury.

IRM 10.8.1 and the *IRS System Security Plan for Taxpayer Digital Communications* require that user accounts be disabled, quarantined, or removed after a specified number of calendar days of inactivity. Specifically, privileged and nonprivileged user accounts should be disabled after 60 and 120 calendar days of inactivity and quarantined after 90 and 240 calendar days of inactivity, respectively. Both privileged and nonprivileged user accounts should be removed after 365 calendar days of inactivity.

The configuration setting "maximum inactivity time frame" on the eGain platform was set to 120 calendar days for disabling user accounts due to inactivity, but it did not account for the different user roles (*i.e.*, privileged, nonprivileged). On behalf of Contact Center Support division management, a contractor stated that, if the maximum time frame for inactivity has been reached, an account is automatically disabled when the user attempts to log back in to the account. However, there is not an automated process to identify and quarantine or remove a user account for inactivity.

Management Action: We notified Contact Center Support division management of the IRM requirements. On April 20, 2022, a Contact Center Support division contractor stated that they will update the configuration setting to be more restrictive for a maximum inactivity time frame of 60 calendar days to disable both privileged and nonprivileged user accounts.

The Chief Information Officer should:

Recommendation 8: Develop a process and ensure adequate oversight is provided to ensure that Contact Center Support division personnel timely disables, quarantines, and removes user accounts for inactivity in accordance with IRM requirements.

> **Management's Response:** The IRS agreed with this recommendation. The IRS and the eGain MSP have changed the user account inactivity parameter from 120 to 60 calendar days on the TDC platform. This will ensure that the Contact Center Support division personnel timely disabled, quarantined, or removed after a specified number of calendar days of inactivity.

Recommendation 9: Ensure that Contact Center Support division personnel, including contractors, are aware of user account management requirements.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will ensure that Contact Center Support division personnel, including contractors, are aware of user account management requirements by updating the *Contact Center Support Division Commercial Off-The-Shelf Users Guide Standard Operating Procedures* and by hosting training to ensure that all personnel are aware of user account management requirements.

Default vendor accounts were re-enabled and test accounts were used in the production environment

We requested and obtained documentation to support when the default vendor accounts were disabled. Our review identified that two default vendor accounts were re-enabled after the TDC platform launched on December 10, 2016. The TDC platform was installed with two default vendor accounts, the partition administrator account and system administrator account. The partition administrator account is used for setting up and managing partitions and system

resources. The system administrator account is used for the installation, maintenance, and security of the system. The eGain MSP Senior Project Manager stated that both default vendor accounts have no production use and that the account names and passwords were not changed when they were originally disabled. In addition, using the same eGain MSP listing of 3,441 users having access to the TDC platform, we identified two test accounts in the production environment that were created to test and troubleshoot the platform. While one test account was never logged in, the other test account was last logged in on December 22, 2020.

IRM 10.8.1 requires that all vendor-supplied infrastructure accounts and passwords that have no production use be changed or disabled as soon as the system or software has been installed. In addition, the IRS provides that developers do not develop or test on production systems. All systems should be tested prior to being placed into the production environment.

The eGain MSP Senior Project Manager was unable to provide support but stated that both vendor default accounts were initially disabled when the platform was launched. The eGain MSP Senior Project Manager explained that the partition administrator and system administrator accounts were temporarily re-enabled in January 2018 to disconnect a system monitor linked to the partition administrator account so the monitor could be used and in August 2020 to apply a system security patch to fix a bug in the software. At that time, system limitations prevented the actions required without re-enabling the two vendor default accounts. On behalf of Contact Center Support Division management, a contractor also stated that "if there is a new deployment of a package in (the) production environment, it is standard practice that the vendor tests basic functionality works in production once a release of a new package has gone live."

Re-enabling default vendor accounts and not changing or disabling passwords and having test accounts in the production environment unnecessarily exposes the TDC and eGain platforms to unauthorized access, which may result in damage or data loss.

After we discussed these items with the IRS, the Federal Information Security Modernization Act Processes and Controls Management Cloud team conducted a Cloud-Security Assessment and Authorization assessment. We reviewed the assessment documentation in which the IRS determined that default vendor accounts are changed or disabled, and appropriate account management practices (*i.e.*, not using test accounts) are being followed in accordance to IRM requirements.

Passwords settings for local user accounts are set to never expire

While the majority of user accounts are accessed using single sign-on, we identified 52 local user accounts that are accessed using a username and password. Local user accounts include both administrator and analyst type accounts and are used to perform troubleshooting, validate software updates, and provide technical support to users and taxpayers. Our review determined that the passwords for 10 (19.2 percent) of the local user accounts had not been changed in over 60 calendar days. The number of days late ranged from 61 to 944 calendar days, averaging 154 calendar days.

IRM 10.8.24 requires users to change their passwords every 60 calendar days. A review of the password settings determined that they were left at the default setting and not configured (*i.e.*, the fields for the password settings were set at zero calendar days). On behalf of Contact Center Support division management, a contractor explained that the setting for password

expiration does not exist for some local user accounts. However, our review determined that the limitation only applies to two of the 10 local user accounts. By not enforcing password expiration limits, the IRS allows an attacker the time to compromise a user's password and have access to taxpayer data.

The Chief Information Officer should ensure that:

Recommendation 10: Password settings for local user accounts are configured to expire in accordance with IRM requirements.

> **Management's Response:** The IRS agreed with this recommendation. The IRS disabled local user accounts and converted them with single sign-on or personal identity verification card access, except for a limited number of preapproved fire call accounts. The IRS and the eGain MSP implemented updates on the TDC platform to ensure that local login account passwords are disabled if the user has not changed their password after 60 calendar days. The *IRS System Security Plan for Taxpayer Digital Communications* will be updated to reflect the new requirements.

Recommendation 11: A process is developed to identify and enforce that passwords are changed in accordance with IRM requirements for local user accounts for which the password control cannot be applied.

> **Management's Response:** The IRS agreed with this recommendation. The IRS and the eGain MSP implemented controls on the TDC platform so local login account passwords are disabled if the user has not changed their password after 60 calendar days. The IRS will disable almost all local user accounts and convert them with single sign-on or personal identity verification card access, except for a few preapproved fire call (to allow for local login) accounts. The *IRS System Security Plan for Taxpayer Digital Communications* will be updated to reflect the new requirements.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to assess the security and access controls of the TDC platform. To accomplish our objective, we:

- Reviewed Federal and IRS policies, procedures, and guidance on cloud service requirements and interviewed Cybersecurity, Enterprise Services, and User and Network Services functions' personnel to identify their efforts in monitoring, assessing, and ensuring that the eGain platform and the AWS GovCloud's security posture meet those requirements.
- Determined whether the FedRAMP authorizations for the eGain platform and the AWS GovCloud are current and active and security reviews for continuous monitoring are being conducted as well as whether security controls are in place in the areas of encryption; virus protection; system and configuration scanning, vulnerability remediation, and patching; and audit trails by reviewing documentation and interviewing Cybersecurity function and eGain MSP personnel.
- Determined whether security vulnerabilities were timely remediated by reviewing an eGain platform report that contained 177 security vulnerabilities discovered from July 2016 through February 4, 2022. In addition, we reviewed a judgmental sample[1] of 11 security vulnerabilities and their respective vulnerability scans to determine whether the issue ticket creation date is the vulnerability discover date. We selected a judgmental sample because we did not plan to project the results to the population.
- Determined the effectiveness of access controls in the areas of user authorizations and recertifications, the principle of least privilege, password policies, and accounts maintenance by reviewing user account data from a BEARS listing of 3,258 users with authorizations to the TDC platform as of January 6, 2022, and from an eGain MSP listing of 3,441 users having access to the platform as of February 4, 2022.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity, Enterprise Services, and User and Network Services functions located at the New Carrollton Federal Building in Lanham, Maryland, during the period August 2021 through June 2022. 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 Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Nicholas Reyes, Acting Audit Manager; Catherine Sykes, Acting Audit Manager; David F. Allen, Lead Auditor; and Carreen Diaz, Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the BEARS and the eGain MSP. We evaluated the data by 1) reviewing existing information about the data and the systems that produced them; 2) interviewing agency officials knowledgeable about the data; 3) performing electronic testing of required data elements, including that all fields requested were received and record counts equaled to what was expected; and 4) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data. 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: General Services Administration guidance on FedRAMP requirements as well as various Federal and IRS policies and procedures related to security and access controls. We evaluated these controls by interviewing Cybersecurity, Enterprise Services, and User and Network Services functions' personnel concerning the implementation and maintenance of system security and account access and reviewing relevant documentation.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Protection of Resources – Actual; 43 production servers on which the TDC platform resides with two critical and three high severity rated antivirus software releases not installed (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We obtained screenshots of the eGain MSP's dashboard to identify the version of the antivirus software running on the eGain platform and conducted research on the antivirus software vendor website to identify the most current version of the antivirus software available. Our comparison of the antivirus software versions determined that eGain MSP personnel did not install two critical and three high severity rated antivirus software releases, which potentially affected 43 production servers on which the TDC platform resides.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 15 security vulnerabilities that did not include a severity rating of critical, high, medium, or low (see Recommendations 4 and 5).

Methodology Used to Measure the Reported Benefit:

We requested and received a report that identified all security vulnerabilities discovered on the eGain platform from July 2016 through February 4, 2022, to determine whether they were timely remediated. Fifteen of the security vulnerabilities did not include a severity rating of critical, high, medium, or low.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 498 incorrect authorizations for users with authorizations in the BEARS who did not have access to the TDC platform (see Recommendation 7).

Methodology Used to Measure the Reported Benefit:

We requested and obtained user account data from the BEARS, a listing of 3,258 users with authorizations to the TDC platform as of January 6, 2022, and from the eGain MSP, a listing of 3,441 users having access to the TDC platform as of February 4, 2022. We reviewed and compared the two listings and determined that, of 3,939 distinct total users, 498 users with authorizations in the BEARS did not have access to the TDC platform.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 681 users who have access to the TDC platform but did not have authorizations in the BEARS (see Recommendation 7).

Methodology Used to Measure the Reported Benefit:

We requested and obtained user account data from the BEARS, a listing of 3,258 users with authorizations to the TDC platform as of January 6, 2022, and from the eGain MSP, a listing of 3,441 users having access to the TDC platform as of February 4, 2022. We reviewed and compared the two listings and determined that, of 3,939 distinct total users, 681 users who have access to the TDC platform did not have authorizations in the BEARS.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 8, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer
Kaschit D. Pandya Digitally signed by Kaschit D. Pandya
Date: 2022.09.08 13:54:59 -04'00'

SUBJECT: Response to Draft Report – Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened (Audit #202220014)

Thank you for the opportunity to review and comment on the draft report. The Taxpayer Digital Communications (TDC) initiative provides a secure digital environment for taxpayers to interact with the IRS, and we continue to innovate, expand digital communications, and deliver technology with the appropriate security controls in place to protect taxpayer data.

The IRS adheres to the governmentwide standards for the adoption of secure cloud services, and we use the standardized approach to security assessments, authorizations, and continuous monitoring for cloud products and services as part of the Federal Risk and Authorization Management Program (FedRAMP). In partnership with our cloud service providers, we uphold the shared security responsibilities and remain committed to continuous monitoring and compliance. We are pleased that TIGTA acknowledges that the platform production servers on which the TDC platform resides are encrypted and in compliance with the applicable federal standards and that the platform configuration settings for password length and complexity comply with IRS security policies.

We are committed to further improving security and access controls over the TDC platform and agree with the recommendations in this report. We agree with the outcome measures and will address them along with the associated recommendations outlined in our corrective action plan. Administrative, procedural, and documentation improvements will be implemented to further increase the security posture of the TDC platform, as noted in the corrective action plan. We note that many of the actions needed to address the audit team's findings were already in progress at the time of the report's drafting or have already been completed.

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 Kevin McCreight, Contact Center Support division director, at 470-769-5069.

Attachment

Attachment

Audit# 202220014, *Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened*

Recommendation 1: The IRS Chief Information Officer (CIO) should ensure that IRS Cloud Continuous Monitoring Strategy Standard Operating Procedures is updated requiring that security reviews for continuous monitoring begin when the CSP is first FedRAMP authorized.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. IRS will update the Cloud Continuous Monitoring Strategy Standard Operating Procedure (SOP) to require that continuous monitoring begins when a CSP (Cloud Service Provider) is first FedRAMP authorized.

IMPLEMENTATION DATE: December 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 2: The IRS CIO should ensure that FedRAMP security reviews for continuous monitoring are conducted to ensure that the AWS GovCloud's security posture remains sufficient for the TDC platform.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Annual Security Control Assessment (ASCA) for eGain (TDC commercial implementation) was completed on May 4, 2022 and will be conducted each year hence forth. This action ensures that the AWS GovCloud's security posture remained sufficient as part of the FedRAMP security review for continuous monitoring.

IMPLEMENTATION DATE: December 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 3: The IRS CIO should ensure that adequate oversight is provided to ensure that eGain MSP personnel timely upgrade antivirus software in accordance with IRM requirements.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS now requires that eGain MSP provide weekly patching and anti-virus definition updates to include timeliness reporting. The eGain MSP provides a monthly summary of the

patching and anti-virus definition updates report in the monthly report to the IRS. The Taxpayer Digital Communications System Security Plan (TDC SSP) will be updated to reflect this requirement.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 4: The IRS CIO should ensure that management oversight is provided to ensure that the eGain MSP timely remediates identified security vulnerabilities in accordance with the remediation time frames for Internet accessible systems.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS has implemented this recommendation and receives a weekly report from eGain MSP that verifies all patching and security vulnerabilities are being addressed. The TDC SSP will be updated to reflect the new requirement.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 5: The IRS CIO should ensure that the *IRS System Security Plan* for Taxpayer Digital Communications is updated to reflect the correct vulnerability remediation time frame and that the TDC platform is an Internet accessible system.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The patching process has been implemented, and the scanning schedule now occurs weekly. The TDC SSP will be updated to reflect that the platform is an Internet accessible system.

IMPLEMENTATION DATE: February 15, 2023

Attachment

Audit# 202220014, *Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened*

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 6: The IRS CIO should ensure that the Counter Insider Threat Operations branch starts reviewing the audit trails for the TDC platform.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Annual Security Control Assessment (ASCA) for eGain (TDC commercial implementation) was completed on May 4, 2022 and identified that that the audit trail capture was not functioning as required. The IRS remediated issue and the audit log capture resumed prior to the end of May 2022. The IRS Counter Insider Threat Operations branch will continuously monitor eGain audit trails per IRM guidelines.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 7: The IRS CIO should reconcile between users having authorizations in the BEARS and users having access to the TDC platform, and resolve any discrepancies identified by adding or removing the authorization or user account based upon whether there is a business need for access.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS will review BEARS entitlements access to ensure they align with eGain systems access and address discrepancies for user entitlement authorizations. The IRS Business Units will be required to provide quarterly account reconciliation reports and IRS IT will review the quarterly BEARS reports to reconcile with eGain reports for continuity.

IMPLEMENTATION DATE: April 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Audit# 202220014, *Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened*

Recommendation 8: The IRS CIO should ensure that develop a process and ensure adequate oversight is provided to ensure that Contact Center Support Division (CCSD) personnel timely disables, quarantines, and removes user accounts for inactivity in accordance with IRM requirements.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS and eGain MSP have changed the user account inactivity parameter from 120 days to 60 days on the TDC platform. This will ensure that the *Contact Center Support Division (CCSD) personnel timely* disabled, quarantined, or removed after a specified number of calendar days of inactivity.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 9: The IRS CIO should ensure that Contact Center Support Division (CCSD) personnel, including contractors, are aware of user account management requirements.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The ASCA for the TDC platform was completed on May 4, 2022. The assessment documentation demonstrated the IRS is satisfying the controls for this recommendation. The IRS will also ensure that Contact Center Support Division (CCSD) personnel, including contractors, are aware of user account management requirements by updating the CCSD COTS Users Guide Standard Operating Procedures (SOP) and by hosting training to ensure all personnel are aware of user account management requirements

IMPLEMENTATION DATE: December 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Audit# 202220014, *Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened*

Recommendation 10: The IRS CIO should ensure that password settings for local user accounts are configured to expire in accordance with IRM requirements.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS disabled local user accounts and converted them with SSO/PIV Card access except for a limited number of pre-approved Fire Call accounts. The IRS and the eGain MSP implemented updates on the TDC platform to ensure local login account passwords are disabled if the user has not changed their password after 60 days. The TDC SSP will be updated to reflect the new requirements.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Recommendation 11: A process is developed to identify and enforce, that passwords are changed in accordance with IRM requirements for local user accounts for which the password control cannot be applied.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS and eGain MSP implemented controls on the TDC platform so local login accounts password is disabled if the user has not changed password after 60 days. The IRS will disable almost all local user accounts and convert them with SSO/PIV Card access, except for a few pre-approved Fire Call (to allow for local login) accounts. The TDC SSP will be updated to reflect the new requirements.

IMPLEMENTATION DATE : February 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Appendix IV

Glossary of Terms

Term	Definition
Agent	Conducts examinations of individuals, businesses, corporations, and Government entities to determine Federal tax liability.
Antivirus Software	Scans computer files and memory to detect and eradicate malicious code.
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Authentication	The process by which a system verifies the identity of a user who wishes to access it.
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.
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Credential Service Provider	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A credential service provider may be an independent third party or issue credentials for its own use.
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.
Default Vendor Account	A user account already created on the operating system that allows a system administrator to make changes to the system. The system administrator can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.
Encryption	The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents.
Engagement Hub	A customer engagement platform that improves customer experience and contact center performance.
Installation	Software placed on a medium from which it can be executed.
Malicious Code	Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, Trojan horses, and malicious data files.

Term	Definition
Managed Service Provider	A third-party company that remotely manages a specified set of information technology processes, such as security, infrastructure, maintenance, support, *etc.*, for end-user systems.
Nonprivileged	Any user right assignment that is at the organization's baseline.
Partition	A logical portion of a media that functions as though it were physically separate from other logical portions of the media.
Patch	An immediate solution to remediate identified vulnerabilities, it is a small file provided to users that will fix a specific vulnerability when executed.
Portal	A standard secure connection to a website that allows a remote user to securely access multiple network services using a standard web browser.
Privileged	Any user right assignment that is above the organization's baseline for regular users. Sometimes referred to as system or network administrative accounts.
Single Sign-On	Provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various target systems. Target applications and systems still maintain their own credential stores and present sign-on prompts to client devices. Behind the scenes, single sign-on responds to those prompts and maps the credentials to a single login and password pair.
Software-as-a-Service	Software that is provided by an independent vendor and typically hosted on the cloud.
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. May have the capability to corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a computer hard disk drive.
Vulnerability	A bug, flaw, weakness, or exposure in an information system, software, or application that could be exploited and lead to failure, resulting in loss of confidentiality, integrity, or availability.

Appendix V

Abbreviations

AWS	Amazon Web Services
BEARS	Business Entitlement Access Request System
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
MSP	Managed Service Provider
TDC	Taxpayer Digital Communications

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

(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.