TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed

May 18, 2022

Report Number: 2022-27-028

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

HIGHLIGHTS: The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed

Final Audit Report issued on May 18, 2022 **Report Number 2022-27-028**

Why TIGTA Did This Audit

On March 11, 2021, the President signed the American Rescue Plan Act of 2021 into law, which required the IRS to establish a Child Tax Credit (CTC) Advance Payment Program. In response to this requirement, the IRS developed the CTC Update Portal, which was deployed on June 21, 2021.

This audit was initiated to assess the IRS requirements review process and the development of the CTC Update Portal, including any impacted or associated systems and applications.

Impact on Tax Administration

On July 15, 2021, the IRS issued the first round of advance CTC payments totaling $15 billion to 35 million taxpayers and impacting more than 60 million children. As of October 30, 2021, the IRS had generated 142.8 million CTC payments totaling $61 billion.

In addition, as part of the CTC Update Portal development, the IRS accelerated the initial launch of the Secure Access Digital Identity (SADI) system from a small-scale pilot program to a full-scale production solution that will serve as its next-generation identity proofing solution to improve taxpayer access to online services.

Implementing both the CTC Update Portal and SADI system will improve taxpayer services and the security of taxpayer data accessed through online applications.

What TIGTA Found

The Enterprise Life Cycle process was generally effective in ensuring that both the CTC Update Portal and SADI system met accelerated deployment timelines in order to meet legislative requirements. The Security Risk Management organization took management action to revise the Milestone Exit Memorandum template to provide explicit concurrence for systems to operate in the production environment. In addition, due to a communication issue, a cloud service provider's solution was implemented without having an agency-issued Authorization to Operate. The IRS appropriately assessed and implemented the CTC Update Portal's identity, authenticator, and federated assurance levels.

The IRS implemented 311 (87 percent) of 356 applicable security controls for the CTC Update Portal and SADI system, but the Privacy, Governmental Liaison, and Disclosure organization does not have a formal documented process to manage the selection, implementation, and assessment of privacy controls.

The IRS failed to timely remediate 1,818 critical (356 unique), six high (all unique), and two medium (all unique) security vulnerabilities that were identified in either the CTC Update Portal or SADI system. In addition, 199 (96 percent) of 207 CTC Update Portal and SADI system servers were noncompliant due to either failing a high-compliance check or having weighted compliance scores of less than 90 percent. The IRS stated that the root cause of the remediation findings stemmed from older software versions being installed during the server build process. Finally, an administrative oversight related to server monitoring resulted in a CTC Update Portal outage for approximately 28 hours.

What TIGTA Recommended

TIGTA made 10 recommendations, including that the Chief Information Officer ensure that Enterprise Life Cycle coaches comply with existing agency requirements related to the independent verification and validation; establish a validation process so that all required physical, environmental, and media protection controls are implemented; ensure that Plans of Action and Milestones are completed timely; ensure that IRS systems supported by cloud service providers have an approved Authorization to Operate prior to deployment; and validate that newly built servers meet minimum compliance requirements during the server build process. In addition, the Chief Privacy Officer should ensure that formal documentation is created that provides evidence that all privacy controls were properly selected, implemented, and assessed.

The IRS agreed with all 10 recommendations and responded that it implemented corrective actions for six of the 10 recommendations. In addition, the IRS plans to ensure that all SADI system Plans of Action and Milestones are completed timely, and prioritize remediation efforts for two noncompliant SADI system servers.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 18, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed (Audit # 202120722)

This report presents the result of our review to assess the Internal Revenue Service (IRS) requirements review process and the development of the Child Tax Credit Update Portal, including any impacted or associated systems and applications. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Administration of Tax Law Changes and Pandemic Relief Benefits*.

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

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 ..... Page 1

Results of Review ..... Page 1

Most Enterprise Life Cycle Artifacts Satisfied IRS Requirements ..... Page 1

Recommendations 1 through 3: ..... Page 4

The Cloud Service Provider's Solution Was Implemented Without an Approved Authorization to Operate Letter ..... Page 4

Recommendation 4: ..... Page 5

The Digital Identity Acceptance Statement Met Both Federal and IRS Security Requirements ..... Page 5

Most Required Security Controls Were Implemented ..... Page 7

Recommendations 5: ..... Page 11

Recommendations 6 and 7: ..... Page 12

Security Vulnerabilities Were Not Timely Remediated ..... Page 12

Recommendation 8: ..... Page 14

Configuration Compliance Controls Are Insufficient ..... Page 15

Recommendations 9 and 10: ..... Page 16

An Administrative Oversight Resulted in an Extended Portal Outage ..... Page 16

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 18

Appendix II – Summary of Associated Plans of Action and Milestones ..... Page 20

Appendix III – Summary of Risk-Based Decisions Associated With the Secure Access Digital Identity System ..... Page 22

Appendix IV – Management's Response to the Draft Report ..... Page 23

Appendix V – Glossary of Terms ..... Page 30

Appendix VI – Abbreviations ..... Page 33

Background

On March 11, 2021, the President signed the American Rescue Plan Act of 2021 into law.[1] This Act created Internal Revenue Code § 7527A, which requires the Secretary of the Treasury to establish the Child Tax Credit (CTC) Advance Payment Program. In response to this requirement, the Internal Revenue Service (IRS) developed the CTC Update Portal, which was deployed on June 21, 2021. As of November 1, 2021, more than 6.6 million taxpayers registered to use the portal. The CTC Update Portal allows taxpayers to elect out of receiving payments related to the advance CTC as well as to provide updates to the number of qualifying children, marital status, or significant change in the taxpayer's income.

On July 15, 2021, the IRS issued the first round of advance CTC payments totaling $15 billion to 35 million taxpayers and impacting more than 60 million children. As of October 30, 2021, the IRS generated 142.8 million CTC payments totaling $61 billion. In addition, as part of the CTC Update Portal development, the IRS accelerated the initial launch of the Secure Access Digital Identity (SADI) system from a small-scale pilot program to a full-scale production solution that will serve as the IRS's next-generation identity proofing[2] solution to improve taxpayer access to IRS online services. Implementing both the CTC Update Portal and SADI system will improve taxpayer services and the security of taxpayer data accessed through online applications.

Results of Review

Most Enterprise Life Cycle Artifacts Satisfied IRS Requirements

The Enterprise Life Cycle (ELC) is a defined, developed, and institutionalized proven set of best project management practices for managing change in IRS business processes and systems. The objectives of the ELC framework are to:

- Standardize the approach for managing, governing, and supporting projects following the ELC framework throughout the IRS.
- Improve the probability of successfully achieving desired change within budget, schedule, and scope.
- Help ensure project success by reducing risk and ensuring compliance with applicable internal and external standards and mandates such as the Federal Information Security Modernization Act of 2014.[3]

The Internal Revenue Manual (IRM)[4] states that it is IRS policy to use best practice methodologies, such as the ELC, to document and improve IRS information technology process

[1] Pub. L. No. 117-2, 135 Stat. 4 (codified in scattered sections of 7, 12, 15, 19, 20, 26, 29, 42, and 45 U.S.C.).

[2] See Appendix V for a glossary of terms.

[3] Pub. L. No. 113-283. This Act amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

[4] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (Sept. 28, 2021).

and service efficiency and effectiveness. The IRM[5] also states that the scope of the ELC framework includes systems strategy, architecture, and engineering capabilities across information technology infrastructure, business applications, data management, and information technology security.

The ELC office provides guidance on the implementation of ELC requirements via ELC coaches. ELC coaches are required to conduct independent verification and validation through milestone readiness reviews, during which the ELC coaches review a project's compliance with ELC guidance. In addition, IRS requirements state that all applicable ELC artifacts be listed in the approved Project Tailoring Plan for the individual projects.

We reviewed the Project Tailoring Plans for both the CTC Update Portal and SADI system. The CTC Update Portal's Project Tailoring Plan listed 16 required ELC artifacts. The SADI system's Project Tailoring Plan listed 12 required ELC artifacts. While we found administrative issues with several ELC artifacts, we determined that 15 (94 percent) of the 16 required CTC Update Portal ELC artifacts and 11 (92 percent) of the 12 required SADI system ELC artifacts satisfied IRS requirements. The administrative issues we found included: a tailoring decision incorrectly documented in the CTC Update Portal Project Tailoring Plan; an unauthorized approver granting use of draft artifact; inaccurate security assessments during milestone reviews; artifact owners not timely approving artifacts prior to required milestone reviews; secondary and tertiary proxy approvers not formally documented; and not adhering to IRS artifact submission time requirements. However, the ELC process was generally effective in ensuring that both the CTC Update Portal and SADI system met accelerated deployment timelines in order to meet legislative requirements. Figure 1 summarizes the two ELC artifacts that did not satisfy IRS requirements.

Figure 1: Summary of ELC Artifacts That Did Not Satisfy IRS Requirements

Artifact Name	Artifact Description	Underlying Issues
CTC Update Portal Computer Operators Handbook	Provides all responsible personnel for the operation and support of a solution with operational instructions for supporting daily operations.	• The draft CTC Update Portal Computer Operators Handbook was not completed prior to the CTC Update Portal's Release 1 production deployment date of June 21, 2021. The process owner approved the draft CTC Update Portal Computer Operators Handbook 43 days later on August 3, 2021.
SADI 508 Accessibility and Mitigation Package	Explains the approach and tests to be used to ensure that the solution being developed or implemented will be accessible to users with disabilities and demonstrates compliance via actual test results.	• The process owner did not sign the 508 Package Sign-Off Sheet prior to the SADI system's June 21, 2021, production deployment due to material concerns regarding the number of test procedure failures. The Project team needed additional time to address the concerns and the process owner approved the SADI 508 Accessibility and Mitigation Package on September 7, 2021, 78 days after its production deployment. • Did not adhere to established ELC artifact timelines (completed package not submitted on time).

Source: Treasury Inspector General for Tax Administration (TIGTA) analysis of the CTC Update Portal and SADI system ELC artifacts.

[5] IRM 2.16.1, *Enterprise Life Cycle Guidance* (Aug. 13, 2021).

Based on our evaluation, we determined that the primary contributing factors to each of the causes for the administrative issues identified and the two ELC artifacts not satisfying IRS requirements were related to the accelerated deployment timelines, significantly increased workload, and competing project prioritization. Specific causes included miscommunication and lack of communication between the project team and process owners, lack of quality control due to the absence of independent validation and verification of ELC artifacts by the ELC coach, not adhering to established ELC artifact timelines, and the lack of a formal process to identify primary and proxy approvers of ELC artifacts. By not adhering to the approved ELC process, to include meeting minimum ELC artifacts requirements, the projects did not comply with IRS guidelines and overall goals.

Milestone exit memorandum

As part of the ELC process, the Cybersecurity function's Security Risk Management (SRM) organization is required to provide the system's authorizing official a Milestone Exit Memorandum. This memorandum provides a list of the security artifacts that were included as part of the review, any artifacts that require additional work, and an exit recommendation. The Director of the SRM organization signed conditional Milestone Exit Memorandums for both the CTC Update Portal and SADI system.[6]

Both memorandums included language that stated, "Cybersecurity will conduct a final review and concur with mitigated findings from outstanding critical risks resulting from security scanning, and Cybersecurity will provide concurrence to go live." When asked if the Cybersecurity function provided this concurrence for the CTC Update Portal and SADI system to go live, management officials from the SRM organization stated that the information was contained on the signature page on each system's Preliminary Security Analysis Report. Our review of these documents did not find any evidence in which the Cybersecurity function provided explicit concurrence for either the CTC Update Portal or SADI system to operate in the production environment. In a following discussion, the SRM organization stated that the appropriate documentation was completed, but acknowledged that the memorandum template required updated language to reflect the current process in order to provide explicit concurrence to operate in the production environment.

By providing system authorizing officials with explicit concurrence to operate in the production environment, there is minimal risk that critical and high-risk security findings might not have been mitigated or that the authorizing officials are basing their decision to grant an Authorization to Operate (ATO) on inaccurate or outdated information.

Management Action: On January 28, 2022, the IRS revised the language contained in the Milestone Exit Memorandum template to accurately align with the current process for the SRM organization to provide explicit concurrence to operate in the production environment.

[6] The CTC Update Portal's memorandum was not signed until 6.5 hours after the Web Applications Governance Board voted unanimously to approve the CTC Update Portal's milestone exit.

The Chief Information Officer should:

Recommendation 1: Ensure that the ELC coaches comply with existing agency requirements related to the independent verification and validation of all ELC artifacts.

> **Management's Response:** The IRS agreed with this recommendation. The recommendation is a part of the ELC Process; however, this was an internal error that will be addressed going forward ensuring compliance, following process and procedure as outlined in the IRM.

Recommendation 2: Ensure that only authorized approving authorities provide status updates and grant final approval of ELC artifacts during required milestone reviews.

> **Management's Response:** The IRS agreed with this recommendation. The recommendation is a part of the ELC Process. To remediate the recommendation, the IRS implemented a detailed *ELC Required Artifacts Process Owner Approver Listing* and briefed the ELC coaches on their role to ensure compliance with ELC standard requirements.

Recommendation 3: Establish a formal process, which includes routine updates, to identify primary and proxy approvers for all ELC artifacts.

> **Management's Response:** The IRS agreed with this recommendation. The recommendation is a part of the ELC Process. To remediate the recommendation, the IRS implemented a *Process Owner Meetings Standard Operating Procedure* and a detailed *ELC Required Artifacts Process Owner Approver Listing* and briefed ELC coaches on their role to ensure compliance with ELC standard requirements.

The Cloud Service Provider's Solution Was Implemented Without an Approved Authorization to Operate Letter

The Office of Management and Budget requires agencies to authorize an information system prior to operation and periodically thereafter.[7] In addition, the Office of Management and Budget requires that Federal agencies leverage the Federal Risk and Authorization Management Program (FedRAMP) for all cloud-based services.[8] The FedRAMP mandates agencies to issue their own ATO letter to show that the agency is accepting the security risks associated with the cloud service. Lastly, agency requirements state that a Cloud Security Threat Analysis Report must be completed when new IRS programs, project, or information systems intend to require a FedRAMP certified cloud service provider (CSP).

On June 7, 2021, the IRS leveraged an existing Department of the Treasury Blanket Purchase Agreement and issued a delivery order against the Blanket Purchase Agreement for software

[7] Office of Management and Budget, Circular No. A-130, Appendix II, *Responsibilities for Managing Personally Identifiable Information* (July 2016).

[8] Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 2011).

licenses and software maintenance Credential Service Provider[9] to provide identity proofing support. This FedRAMP authorized cloud-based service, along with the CTC Update Portal and SADI system, went live on June 21, 2021.

On June 15, 2021, the Director of the SRM organization signed the completed Cloud Security Threat Analysis Report, which provides the authorizing official with systematic analysis of probable threat characteristics, potential security risks, and the overall security posture of the CSP. However, due to a communication issue, the SRM organization did not timely provide the completed Cloud Security Threat Analysis Report and the CSP's agency ATO letter to the authorizing official.

On June 23, 2021, approximately two days after the CSP went live, the authorizing official ultimately signed both the Cloud Security Threat Analysis Report and the CSP's agency ATO letter, authorizing the CSP to operate for the IRS. Authorization of an information system is an explicit acceptance of the risk to IRS operations, agency assets, individuals, other organizations, and taxpayers based on the implementation of the security and privacy controls. By allowing the CSP's solution to be implemented without an approved agency ATO letter, the IRS cannot ensure that the CSP operates with an acceptable level of risk to IRS operations, IRS assets, other organizations, and taxpayers.

Lastly, on July 7, 2021, approximately 16 days after the SADI system went live, the IRS entered into a separate agreement with the same CSP to provide security services related to audit logging, data security, and providing assistance with fraud analysis and detection. During the 16-day period with no contractual services for fraud analysis and detection, the IRS implemented a manual data retrieval fraud monitoring and analysis process with the CSP to address fraud activity. By not securing contractual security services prior to the CSP solution going live, the IRS was operating with increased risk for unauthorized network access that could result in fraudulent activity or the loss of sensitive taxpayer data. As an example, on July 7, 2021, prior to the services contract being in place, there was a confirmed case of fraud associated with the CSP in which one user account with successful IRS access was hijacked through social engineering.

Recommendation 4: The Chief Information Officer should ensure that systems supported by the CSPs have an approved IRS ATO prior to a system's deployment.

> **Management's Response:** The IRS agreed with this recommendation. The IRS has a robust documented ATO process in place, yet for this instance a one-time user error occurred which is not normal process. The IRS will continue to ensure that the processes are being followed.

The Digital Identity Acceptance Statement Met Both Federal and IRS Security Requirements

In June 2017, the National Institute of Standards and Technology (NIST) updated technical requirements for Federal agencies related to authentication and identity risks associated with implementing digital identity services. Federal agencies must perform risk assessments; select

[9] The Credential Service Provider is ID.me, which provides identity proofing and user authentication through an agreement with contractor V3Gate.

individual assurance levels for identity proofing, authentication, and federation (if applicable); determine which processes and technologies they will employ to meet each assurance level; and document these decisions in a Digital Identity Acceptance Statement. The Digital Identity Acceptance Statement must include the assessed assurance levels, the implemented assurance levels, rationale if the implemented assurance levels differ from the assessed assurance levels, comparability demonstration of compensating controls, and rationale if federated entities are not accepted.

IRS procedures for the Digital Identity Risk Acceptance process implement the risk acceptance methodology required by the NIST.[10] IRS procedures also document the purpose, procedures, and outputs of each activity within the Digital Identity Risk Acceptance process and include three main components: assessment of assurance levels, assurance levels for implementation, and approval and oversight.

We reviewed the Digital Identity Acceptance Statement and all related documents for the CTC Update Portal and found that the IRS appropriately assessed and implemented level two controls for the identity, authenticator, and federated assurance levels. The NIST defines the components of level two identity assurance, authenticator assurance, and federated assurance as follows:

- *Identity Assurance Level Two:* Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. This level also introduces the need for either remote or physically present identity proofing.
- *Authenticator Assurance Level Two:* Provides high confidence that the claimant controls authenticators bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols. Approved cryptographic techniques are required at this level and above.
- *Federated Assurance Level Two:* Adds the requirement that the assertion be encrypted using approved cryptography such that the relying parties are the only parties that can decrypt it.

In addition, existing IRS users with a Secure Access Electronic Authentication account will have the option to use this account during a transition period while the current identity proofing solution, Electronic Authentication (hereafter referred to as e-Authentication), is phased out. In March 2020, we recommended that, once the SADI system platform was released, the IRS implement a plan to migrate all of the online applications from the current system to the SADI system as expeditiously as possible.[11] The IRS agreed with this recommendation and on August 3, 2021, provided a SADI system integration plan that would migrate all applications currently using e-Authentication to the SADI system and decommission e-Authentication by December 2022.

By ensuring that the CTC Update Portal complies with all applicable NIST and IRS security requirements related to digital identity services, the IRS has taken steps to mitigate the risks

[10] IRS, *Digital Identity Risk Assessment Standard Operating Procedures*, Version 1.6 (July 2019).

[11] TIGTA, Report No. 2020-20-012, *While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established* (Mar. 2020).

associated with potential unauthorized access and activities, compromised taxpayer records, and lost revenue due to identity theft and refund fraud.

Most Required Security Controls Were Implemented

NIST guidelines[12] specify security controls for organizations and information systems that support the executive agencies of the Federal Government to ensure that they meet the minimum requirements of the Federal Information Processing Standards.[13] These guidelines apply to all components of an information system that process, store, or transmit Federal information.

The IRM establishes the security framework for the development of security control–specific implementations defined in subordinate IRMs, IRS publications, and other procedural guidance. The IRM also requires that all information systems be assigned a Federal Information Processing Standards Security Impact-Level Designator.[14] Security Impact-Level Designators are:

- (L) – Applies to systems categorized as Impact-Level LOW.
- (M) – Applies to systems categorized as Impact-Level MODERATE.
- (H) – Applies to systems categorized as Impact-Level HIGH.

IRS security policies require that security controls be documented and assessed for a system's initial authorization, updated and assessed annually for a system's continued authorization, and updated and assessed on an ad-hoc basis resulting from significant changes performed on the system.[15]

The CTC Update Portal is part of the Web Applications Enterprise Services information system boundary, which provides a common set of resources comprised of technology, tools, processes, and documentation to facilitate rapid development initiatives to build, deploy, and manage software applications and services. The Web Applications Enterprise Services boundary, including the CTC Update Portal, is designated as a Moderate-Impact system. According to Cybersecurity function officials, the addition of the CTC Update Portal to the Web Applications Enterprise Services boundary was a change to the system and triggered an Event-Driven Security Controls Assessment.

The SADI system, which is fully compliant with all NIST Digital Identity Guidelines[16] and satisfies the Office of Management and Budget requirements for improved identity, credential, and access management, will provide identity proofing and authentication of users for the CTC

---

[12] NIST, Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013). Revision 5 of this publication was released in September 2020. Starting on July 1, 2021, IRS authorizing officials are responsible for ensuring that new Revision 5 requirements are implemented at the system level and documented in System Security Plans. Because the CTC Update Portal's and the SADI system's Security Control Selection scope occurred before July 1, 2021, we used the criteria established in Revision 4.

[13] Department of Commerce, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (Mar. 2006).

[14] Department of Commerce, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

[15] IRS, *Federal Information Security Modernization Act Security Controls Assessment Standard Operating Procedure* (Sept. 30, 2020).

[16] NIST, Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

Update Portal.[17] The SADI system is designated as a Moderate-Impact system. According to Cybersecurity function officials, because SADI is a new information system, a complete Security Assessment and Authorization is required to complete the system's initial authorization.

We determined that 37 NIST and IRS-specific security controls and control enhancements were applicable to the CTC Update Portal. We found that 29 (78 percent) of 37 applicable security controls and control enhancements were implemented. We also determined that 319 NIST and IRS-specific security controls and control enhancements were applicable to the SADI system. We found that 282 (88 percent) of 319 applicable security controls and control enhancements were implemented. Figures 2 and 3 provide a summary of the CTC Update Portal and SADI system security controls implementation.

Figure 2: Summary of CTC Update Portal Security Controls Implementation

Security Control Family	Applicable Security Controls	Security Controls Implemented	Security Controls Not Implemented
Access Control	9	9	0
Audit and Accountability	4	2	2
Configuration Management	3	1	2
Identification and Authentication	10	9	1
Planning	1	0	1
Risk Assessment	4	2	2
Security Assessment and Authorization	1	1	0
System and Communications Protection	1	1	0
System and Information Integrity	4	4	0
Totals	**37**	**29**	**8**

Source: TIGTA analysis of the CTC Update Portal's security controls.

The five control family categories identified in Figure 2 that have security controls not implemented contain specific risk areas that need to be addressed. The IRS has an active Plan of Action and Milestones (POA&M) for each of the five risk areas to reduce these risks, ensure system integrity, and maximize system availability for taxpayers.

Figure 3: Summary of SADI System Security Controls Implementation

Security Control Family	Applicable Security Controls	Security Controls Implemented	Security Controls Not Implemented
Access Control	30	24	6
Accountability, Audit, and Risk Management	8	8	0
Audit and Accountability	18	15	3
Authority and Purpose	2	2	0
Awareness and Training	5	4	1

[17] Office of Management and Budget, Memorandum M-19-17, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management* (May 2019).

Security Control Family	Applicable Security Controls	Security Controls Implemented	Security Controls Not Implemented
Configuration Management	24	21	3
Contingency Planning	21	21	0
Data Minimization and Retention	6	6	0
Data Quality and Integrity	5	5	0
Identification and Authentication	24	19	5
Incident Response	12	12	0
Individual Participation and Redress	6	6	0
Maintenance	8	8	0
Media Protection	9	1	8
Personnel Security	10	9	1
Physical and Environmental Protection	22	21	1
Planning	6	6	0
Program Management	15	15	0
Risk Assessment	8	7	1
Security	2	2	0
Security Assessment and Authorization	10	10	0
System and Communications Protection	23	20	3
System and Information Integrity	23	18	5
System and Services Acquisition	15	15	0
Transparency	5	5	0
Use Limitation	2	2	0
Totals	**319**	**282**	**37**

Source: TIGTA analysis of the SADI system's security controls.

The 37 security controls identified in Figure 3 as being not implemented contained specific risk areas that need to be addressed. For 28 of these controls, the IRS has either an active POA&M or an approved Risk-Based Decision for these risk areas.[18] For the remaining nine controls, the IRS did not satisfy minimum agency requirements for required security control implementation.

Privacy controls

The Office of Management and Budget requires Federal agencies to implement privacy controls, verify that they are operating as intended, continually monitor and assess them, and put procedures in place so that privacy controls remain effective over time. More specifically, agencies are required to implement a privacy control selection and assessment process to ensure continued compliance with privacy requirements and manage privacy risks.

[18] Appendix II and Appendix III provide a status summary of active POA&Ms and Risk-Based Decisions applicable to either the CTC Update Portal or SADI system.

The Privacy, Governmental Liaison, and Disclosure organization manages privacy controls at the IRS. We evaluated several IRS documents to review the assessment and implementation of the privacy controls applicable to the SADI system.[19] Based on our evaluation, we determined that 36 NIST privacy controls and control enhancements were applicable to the SADI system. We determined that each of the 36 applicable privacy controls and control enhancements were implemented. However, that the Privacy, Governmental Liaison, and Disclosure organization is not effectively managing the selection, implementation, and assessment of privacy controls in accordance with Office of Management and Budget directives and IRS security procedures. For example, there was no formal documentation that provided evidence that all privacy controls were properly selected, implemented, and assessed; no linkage between organizational policies and applicable privacy controls; and no routine verification that the entire NIST control, to include control enhancements, was addressed in the implementation decision making.

In July 2021, Privacy, Governmental Liaison, and Disclosure management officials integrated their employees into the SRM organization's Federal Information Security Modernization Act Certification Program Office's process for the security controls assessment for systems processing Personally Identifiable Information. The IRS stated that, in the future, all privacy control assessments will be conducted using approved procedures.

By not having a formal documented process that provides adequate oversight of the selection, implementation, and assessment of privacy controls, the IRS is potentially at risk of being unable to ensure the privacy and security of taxpayers' personal information.

Physical and environmental protection controls

The Facilities Management and Security Services organization manages the physical and environmental protection controls at the IRS. However, the Cybersecurity function is responsible for validating the assessment and implementation of all NIST security controls. Specific details regarding the IRS's assessment and implementation of these controls are documented in IRS Facility Security Plans and are validated through the Audit Management Checklist, a facility risk assessment tool, or physical security assessments. As part of our review of the assessment and implementation of the physical and environmental protection controls applicable to the SADI system, we evaluated several IRS-provided documents[20] and determined that 21 (95 percent) of 22 physical and environmental protection controls were implemented. As a result of not having a process that ensures the assessment and implementation of all required NIST physical and environmental protection controls, the audit team was unable to evaluate and assess one control related to alternate work site operations.

On November 19, 2021, the Facilities Management and Security Services organization provided Facility Security Plans that documented the implementation of IRS-required physical and environmental protection controls. However, the entry for the control related to alternate work site operations was listed as not applicable. NIST states that this control supports the contingency planning activities of organizations and the Federal telework initiative. We determined that the control was applicable to the IRS. In a follow-up conversation with

[19] This evidence included system security plans, security control assessments, the IRM, and documents that linked privacy controls to the SADI system's Privacy and Civil Liberties Impact Assessment.

[20] This evidence included system security plans, security control assessments, the IRM, Facility Security Plans, and documents that provide an overview of the physical and environmental protection control assessment process.

management officials, they stated that they understand that the control is applicable to the agency and will be incorporated into the Cybersecurity Organizational Common Controls program. While Facilities Management and Security Services management officials are continuing efforts to resolve the issue, as of December 16, 2021, we had not received any new evidence supporting the implementation and assessment of the alternate work site operations control.

By failing to have a process that ensures the assessment and implementation of all required NIST physical and environmental protection controls, the IRS risks being unable to deliver a safe, secure, and optimal work environment that promotes effective tax administration.

Media protection controls

The Enterprise Operations function's Data Storage and Protection Branch is responsible for the implementation and maintenance of media protection controls for IRS systems. However, the SRM organization is responsible for validating the assessment and implementation of all NIST security controls. As part of our review of the assessment and implementation of the media protection controls applicable to the SADI system, we evaluated several IRS-provided documents[21] and determined that eight (89 percent) of nine media protection controls were not implemented per agency requirements.

When asked to provide evidence supporting the implementation and assessment of the media protection controls, management officials from the Information Technology Media Management organization and the SRM organization stated that prior to October 1, 2020, the Facilities Management and Security Services organization documented media protection controls on behalf of the Enterprise Operations function's Data Storage and Protection Branch within IRS Facility Security Plans. However, on October 1, 2020, the Facilities Management and Security Services organization stopped documenting media protection controls within the Facility Security Plans due to the belief that the responsibility for assessing, implementing, and documenting these controls belonged to the Data Storage and Protection Branch. In addition, the SRM organization has begun discussions with the Facilities Management and Security Services organization to reevaluate the media protection controls based on NIST standards to determine: 1) which group will be responsible for identifying ownership of these control requirements, 2) how the implementation will be documented, and 3) who will be tasked with ensuring that these controls are operating as intended.

As a result of not having a process that ensures the assessment and implementation of all required NIST media protection controls, the IRS is unable to provide a full cadre of safeguards and countermeasures for IRS systems.

Recommendation 5: The Chief Privacy Officer should establish a process that complies with Office of Management and Budget requirements regarding the selection, implementation, assessment, and continuous monitoring of privacy controls.

> **Management's Response:** The IRS agreed with this recommendation. The Privacy Compliance and Assurance operation in the Privacy, Governmental Liaison, and Disclosure organization has established a process that is integrated with the IRS

[21] This evidence included system security plans, security control assessments, and the IRM.

Cybersecurity function assessments of NIST controls. This process provides for the selection, implementation, assessment, and continuous monitoring of privacy controls.

Recommendation 6: The Chief Privacy Officer should ensure that formal documentation is created that shows that all the privacy controls applicable to the SADI system are properly selected, implemented, and assessed.

Management's Response: The IRS agreed with this recommendation. The IRS will ensure that formal documentation is created that shows that all the privacy controls applicable to the SADI system are properly selected, implemented, and assessed.

Recommendation 7: The Chief Information Officer should ensure that the Cybersecurity function validates that all required NIST physical and environmental protection and media protection controls are implemented.

Management's Response: The IRS agreed with this recommendation. The IRS will validate all required NIST physical and environmental and media protection controls are documented and assessed to reflect implementation status.

Security Vulnerabilities Were Not Timely Remediated

To satisfy the NIST security control requirement for Vulnerability Scanning (Risk Assessment control family), the IRM requires system owners to deploy vulnerability scanning tools that look for software flaws and improper configuration settings and measure vulnerability impacts. The IRM also requires information systems to be scanned at least monthly for vulnerabilities. We found that the IRS has successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities for both the CTC Update Portal and SADI system. The IRM also states that legitimate vulnerabilities shall be remediated in accordance with IRS-approved response times based on the severity level of the vulnerability. Vulnerabilities with the highest risk shall be prioritized and remediated first. Common Vulnerability Scoring System scores provided by the scanning tools shall be used to prioritize vulnerabilities. Figure 4 shows the score ranges and their associated remediation time frames.

Figure 4: Vulnerability Severity Rating Scale and Remediation Time Frames

Vulnerability Severity Level	Expected Remediation Time Frame
Critical	Internet Accessible Systems Identified in Cyber Hygiene Reports[22] – 15 days All Other Systems – 30 days
High	Internet Accessible Systems Identified in Cyber Hygiene Reports – 30 days High Value Assets – 60 days All Other Systems – 90 days
Medium	120 days
Low	180 days

Source: IRM 10.8.1.

Figure 5 shows a summary of security vulnerabilities for both the CTC Update Portal and SADI system and their associated severity level rating that were past the remediation time frames as of August 10, 2021.

Figure 5: CTC Update Portal and SADI System Vulnerabilities That Exceeded IRS Policy for Remediation

Source: TIGTA analysis of CTC Update Portal and SADI system vulnerabilities as of August 10, 2021.

For the CTC Update Portal, we found that 1,334 (312 unique) critical vulnerabilities spread across nine production servers exceeded the IRS policy for timely remediation. In addition, in the August 2021 CTC Update Portal Security Assessment Report,[23] the SRM organization issued a finding to the Web Applications Enterprise Services authorizing official stating that vulnerability

[22] A weekly report provided by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Cyber Hygiene leverages the Common Vulnerability Scoring System.

[23] IRS, *CTC Update Portal Tier 3 Security Assessment Report* (Aug. 12, 2021).

scan reports identified 412 critical and 508 high-severity security vulnerabilities. In response to this finding, the Enterprise Operations function documented a POA&M with a planned completion date of December 1, 2022.

For the SADI system, we found that 492 vulnerabilities spread across 14 production servers exceeded the IRS policy for timely remediation. Specifically, our analysis of the vulnerability scan report found the following:

- 484 (44 unique) critical vulnerabilities spread across 11 production servers that exceeded the IRS policy of 30 calendar days for remediation.
- 6 unique high vulnerabilities spread across two production servers that exceeded the IRS policy of 90 calendar days for remediation.
- 2 unique medium vulnerabilities impacting one production server that exceeded the IRS policy of 120 calendar days for remediation.

When asked why the 492 vulnerabilities were not remediated within IRS-defined timelines, a management official from the Enterprise Operations function's Authorizing Official Management Branch stated that the root cause of the findings stemmed from older versions of commercial off-the-shelf software being installed during the server build process. In response to this issue, the Enterprise Operations function is developing a process to validate that newly built servers meet minimum compliance requirements. In addition, the Enterprise Operations function is working with the Cybersecurity function to initiate vulnerability scanning prior to newly built servers being placed into the production environment. Lastly, the management official stated that the Enterprise Operations function's Security Operations and Standards Division continues to work and track remediation progress as part of the vulnerability remediation management effort. Each of the vulnerabilities that were not timely remediated are being tracked via active POA&Ms with planned completion dates ranging from December 31, 2021, to December 1, 2022.

Failing to timely remediate security vulnerabilities could compromise the security posture of the CTC Update Portal and SADI system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the system.

Recommendation 8: The Chief Information Officer should ensure that the IRS prioritizes completing the processes that will validate newly built servers being placed into the production environment meet minimum compliance requirements and initiate vulnerability scanning and remediation during the server build process.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will implement a process that will validate newly built servers being placed into the production environment meet minimum compliance requirements and initiate vulnerability scanning and remediation during the server build process.

Configuration Compliance Controls Are Insufficient

The IRM specifies that all information systems must develop, document, and maintain a current baseline configuration. Further, the IRM requires the employment of automated capabilities to maintain an up-to-date, complete, accurate, and readily available baseline configuration of information systems. The IRS uses a configuration setting scanning tool to scan for configuration compliance, and the resulting output is transmitted to a dashboard for review.

Per the IRS user guide,[24] hosts, *e.g.*, servers, are considered compliant if their weighted compliance score is 90 percent or higher with no high-severity ratings. In addition, the IRM requires that a POA&M be developed to document the planned remediation actions to correct weaknesses or deficiencies.

Our review of the CTC Update Portal's configuration setting scanning tool dashboard found that 14 (64 percent) of the 22 production servers were noncompliant due to failing a high-risk compliance check related to the NIST Configuration Management security control family.[25] In response to this configuration compliance issue, the IRS documented a POA&M with a planned completion date of February 4, 2022.

For the SADI system, we found that all 185 production servers were noncompliant due to either failing high-risk compliance checks or having weighted compliance scores less than 90 percent. The failed high-risk compliance checks (183 servers) were related to the NIST Configuration Management and the Risk Assessment security control families. The two POA&Ms that were created to track the mitigation of these high-risk configuration compliance issues were completed in November 2021 and are awaiting final validation and closure from the Cybersecurity function. The two remaining servers were noncompliant due to having weighted compliance scores of less than 90 percent based on the total number of failed medium-risk and low-risk compliance checks.

In addition, we found the configuration setting scanning tool report provides limited historical information, such as client last seen dates. Our review of the scan report found the IRS does not keep track of when a configuration compliance issue was first seen or remediated. In September 2021, we reported[26] that, according to the IRS, the client last seen date shows when the configuration setting scanning tool last scanned the server. The IRS further stated the configuration setting scanning tool saves data for only five days and therefore cannot provide information to determine whether vulnerabilities exceed remediation time frames. We asked how vulnerabilities detected by the configuration setting scanning tool are tracked. We confirmed there is no mechanism within the configuration setting scanning tool to track the age of specific vulnerabilities. We recommended that the IRS evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance scanning tool. The IRS agreed with our recommendation.

On November 12, 2021, in response to our follow-up request regarding this recommendation, the IRS stated that the functionality still does not exist and it hopes to have a resolution in place

---

[24] IRS, *Hindustan Computer Limited BigFix Customer Success Manager Dashboard User Guide, Ver. 1.0* (Nov. 19, 2020).

[25] We also found that each of the CTC Update Portal's 22 production servers had a weighted compliance score above 90 percent.

[26] TIGTA, Report No. 2021-20-063, *Enterprise Linux Platform Management Needs Improvement* (Sept. 2021).

by October 15, 2022.[27] Configuration compliance issues that are not remediated can allow an attacker the opportunity to access and control servers. In addition, without configuration compliance issue age tracking capabilities, remediation and prioritization will be inaccurate and inefficient, and servers will remain at risk.

The Chief Information Officer should:

Recommendation 9: Ensure that all CTC Update Portal and SADI system associated POA&Ms (listed in Appendix II) are completed timely based on IRS-defined timelines and processes.

> **Management's Response:** The IRS agreed with this recommendation. The CTC Update Portal POA&Ms have been completed. SADI system application level POA&Ms (listed in Appendix II) will be completed timely based on IRS-defined timelines and processes. The program level POA&Ms will be completed timely based on IRS-defined timelines and processes.

Recommendation 10: Prioritize remediation efforts on the two noncompliant SADI system servers that have weighted noncompliance scores of less than 90 percent.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will prioritize remediation efforts on the two noncompliant SADI system servers that have weighted noncompliance scores. An analysis of the servers indicates an upgrade is required and will involve SADI system project team testing, validation, and production release time.

An Administrative Oversight Resulted in an Extended Portal Outage

On August 8, 2021, the CTC Update Portal experienced a complete system outage for approximately 28 hours due to an administrative oversight related to server monitoring that occurred during the server build process.

As part of the IRS's server build process, the Information Technology Operations Command Center function's Monitoring Solutions Branch is responsible for ensuring that Internet protocol addresses for new servers are added to the ping monitoring list. However, during the CTC Update Portal's server build process, the Monitoring Solutions Branch's attempt to automate this manual process had unintended consequences that resulted in missing the step of adding each server's Internet protocol address to the monitoring list.

On August 8, 2021, multiple IRS servers, to include the CTC Update Portal, were approved for downtime to allow for server patching and system reboots. During this approved downtime, monitoring functions were disabled to prevent ticket generation. Following the maintenance period, monitoring services were re-enabled with the assumption that monitoring would detect if servers were down. As part of the IRS's Infrastructure Monitoring Policy, servers are pinged every five minutes, and a critical event ticket is generated if a server misses two ping cycles. However, the CTC Update Portal's servers failed to properly come back online, and the issue was not detected due to its Internet protocol addresses not being added to the monitoring list. As a

[27] There is an active Planned Corrective Action related to this finding.

result, the CTC Update Portal project team was unaware of the outage until the morning of August 9, 2021.

During the 28-hour CTC Update Portal outage, users of approximately 240,000 unique Internet protocol addresses who successfully authenticated via the SADI system were unable to access the CTC Update Portal's public-facing website.

Management Action: Following the outage, ping monitoring has been deployed to all CTC Update Portal servers to prevent a similar issue from happening in the future. In addition, the Monitoring Solutions Branch is investigating automating the ping monitoring process in an effort to reduce human error.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to assess the IRS requirements review process and the development of the CTC Update Portal, including any impacted or associated systems and applications. To accomplish our objective, we:

- Reviewed the ELC process for systems development, to include analyzing more than 120 ELC artifacts; interviewed key stakeholders from the Enterprise Program Management Office, Applications Development, Cybersecurity, Enterprise Operations, Business Planning and Risk Management, and Privacy Policy and Compliance functions; and reviewed the results from our planning survey to determine if the CTC Update Portal's development effort complied with minimum IRS requirements.
- Reviewed the Digital Identity Risk Assessment Determination, the Digital Identity Risk Assessment Ongoing Assessment, the Digital Identity Risk Assessment Tool Results, and Oversight and Pre-Oversight Voting Concurrence documents to determine whether the CTC Update Portal's Digital Identity Acceptance Statement met minimum Federal and IRS security requirements.
- Reviewed multiple security vulnerability reports, security assessment reports, risk assessment plans, system security plans, and several POA&Ms and Risk-Based Decisions to determine if the systems supporting the CTC Update Portal met minimum baseline security controls established by the NIST and the IRM.
- Reviewed two security vulnerability reports and two configuration compliance setting vulnerability reports and conducted interviews with officials from the Enterprise Operations function to determine whether security and configuration compliance vulnerabilities were timely remediated or mitigated based on IRS-defined timelines and procedures.

Performance of This Review

This review was performed during the period July 2021 through February 2022. Due to the ongoing Coronavirus Disease 2019 pandemic, we conducted all audit work virtually. We held meetings and interviews via teleconference. We worked closely with the Information Technology organization's Enterprise Program Management Office, Applications Development, Cybersecurity, Enterprise Operations, Business Planning and Risk Management, and Privacy Policy and Compliance functions. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Jason McKnight, Audit Manager; Naomi Koehler, Lead Auditor; Mike Curtis, Senior Auditor; Paula Benjamin-Grant,

Auditor; Johnathan Elder, Information Technology Specialist (Data Analytics); and Julia Wood, Information Technology Specialist (Data Analytics).

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: IRM policies related to information technology ELC projects, NIST and IRS requirements for selecting and specifying security controls for organizations and information systems supporting the Federal Government, IRM policies related to information systems security requirements, Federal and agency requirements related to cloud services, and NIST and IRS requirements related to digital identity controls. We evaluated these controls by interviewing IRS employees and analyzing relevant documentation provided by the IRS.

Appendix II

Summary of Associated Plans of Action and Milestones

Control Family (Control Name)	Applicable System	POA&M Number	Planned Completion Date	POA&M Status
Access Control (Least Privilege)	General Support System – 42	42656	12/31/2021	Late[1]
Access Control (Unsuccessful Logon Attempts)	SADI	45483	8/23/2022	In Progress
Access Control (System Use Notification)	SADI	45485	8/23/2022	In Progress
Access Control (Session Lock and Pattern-Hiding Displays)	SADI	45488	8/23/2022	In Progress
Access Control (Session Termination and Audit Generation)	SADI	45489	8/23/2022	In Progress
Access Control (Remote Access)	Program Level[2]	20707	6/15/2022	In Progress
Audit and Accountability (Correlate Audit Repositories)	Program Level	26028	11/30/2022	Late[3]
Audit and Accountability (Content of Audit Records)	SADI	45484	8/23/2022	In Progress
Audit and Accountability (Audit Storage Capacity and Protection of Audit Information)	General Support System – 42	45099	6/22/2022	In Progress
Awareness and Training (Role-Based Security Training)	Program Level	11055	7/30/2021	Late[4]
Configuration Management (Configuration Settings and Automated Central Management/Application/Verification)	General Support System – 42	45105	6/22/2022	In Progress
Configuration Management (Configuration Settings)	Program Level	24368	12/31/2021	Late[5]
Configuration Management (Configuration Settings)	Program Level	40461	2/4/2022[6]	Completed
Identification and Authentication (Out-of-Band Authentication)	Integrated Enterprise Portal	44551	12/30/2022	In Progress
Identification and Authentication (Authenticator Management and Password-Based Authentication)	General Support System – 42	45110	6/22/2022	In Progress

[1] POA&M 42656 is listed as late because the original planned completion date was October 13, 2021.

[2] Program Level is a POA&M that identifies required tasks to fix a weakness associated with findings that affect multiple IRS systems and organizations.

[3] POA&M 26028 is listed as late because the original planned completion date was July 31, 2021.

[4] POA&M 11055 is listed as late because the original planned completion date was June 30, 2017.

[5] POA&M 24368 is listed as late because the original planned completion date was May 31, 2019.

[6] POA&M 40461 was completed on November 18, 2021, but as of December 6, 2021, the Cybersecurity function has not validated the POA&M for final closure.

Control Family (Control Name)	Applicable System	POA&M Number	Planned Completion Date	POA&M Status
Planning (System Security Plan)	Web Applications Enterprise Services	45346	12/31/2021[7]	Completed
Personnel Security (Personnel Sanctions)	Program Level	22535	12/31/2021	Completed[8]
Risk Assessment (Update by Frequency/Prior to New Scan/When Identified)	Program Level	45244	8/15/2022	In Progress
Risk Assessment (Vulnerability Scanning and Update by Frequency/Prior to New Scan/When Identified)	Program Level	36848	2/28/2025	In Progress
Risk Assessment (Vulnerability Scanning)	Program Level	44695	5/20/2024[9]	Completed
System and Communications Protection (Cryptographic Protection)	General Support System – 42	45113	6/22/2022	In Progress
System and Information Integrity (Flaw Remediation)	SADI	45487	8/23/2022	In Progress
System and Information Integrity (Flaw Remediation)	Program Level	44611	5/9/2022	In Progress
System and Information Integrity (Flaw Remediation)	Program Level	44422	12/1/2022	In Progress
System and Information Integrity (Flaw Remediation)	Program Level	44739	5/26/2022	In Progress
System and Information Integrity (Software, Firmware, and Information Integrity and Integrity Checks and Integration of Detection and Response)	Program Level	16378	11/15/2022[10]	Completed

Source: TIGTA analysis of active IRS POA&Ms.

[7] POA&M 45346 was completed early on December 7, 2021, but as of January 19, 2022, the Cybersecurity function has not validated the POA&M for final closure.

[8] POA&M 22535 was completed on September 28, 2021, but as of January 20, 2022, the Cybersecurity function has not validated the POA&M for final closure.

[9] POA&M 44695 was completed early on November 18, 2021, but as of December 6, 2021, the Cybersecurity function has not validated the POA&M for final closure.

[10] POA&M 16378 was completed early on September 3, 2021, but as of December 6, 2021, the Cybersecurity function has not validated the POA&M for final closure.

Appendix III

Summary of Risk-Based Decisions Associated With the Secure Access Digital Identity System

Control Family (Control Name)	Applicable System	Risk-Based Decision Number	Original Approval Date	Risk-Based Decision Status
Configuration Management (Least Functionality)	General Support System – 42	11205597	9/9/2020	Active
Identification and Authentication (Identifier Management)	General Support System – 42	10660770	5/20/2020	Active
Identification and Authentication (Cryptographic Module Authentication)	Integrated Enterprise Portal	9776768	5/5/2016	Active
System and Communications Protection (Transmission Confidentiality and Integrity)	General Support System – 42	9776897	10/12/2018	Active
System and Communications Protection (Cryptographic or Alternate Physical Protection)	General Support System – 42	9932691	8/15/2019	Active
System and Information Integrity (Central Management)	Integrated Enterprise Portal	9776758	10/19/2015	Active

Source: TIGTA analysis of approved Risk-Based Decisions.

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 3, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer

Nancy A. Sieger
Digitally signed by Nancy A. Sieger
Date: 2022.05.03 10:37:14 -04'00'

SUBJECT: The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed (TIGTA Audit #202120722)

Thank you for the opportunity to review and comment on the draft audit report. We appreciate the acknowledgement that the IRS was effective in meeting the legislative requirements to deploy Child Tax Credit (CTC) Update Portal and accelerated deployment timelines to launch the tool using an improved online authentication experience.

The CTC Update Portal is a secure, password-protected tool that meets all applicable security and privacy requirements. We deployed the tool to help eligible families manage advance CTC payments and followed a proven set of best project management practices as part of the standard Enterprise Life Cycle process to reduce risk and ensure compliance with applicable internal and external standards and mandates. On July 15, 2021, the IRS issued the first round of advance CTC payments totaling $15 billion to 35 million taxpayers and impacting more than 60 million children. As of October 30, 2021, the IRS had generated 142.8 million CTC payments totaling $61 billion.

Generally, the administrative errors that occurred during the rapid deployment of this program have been addressed and/or mitigated by our robust and multi-layered cybersecurity program. The IRS implemented 311 (87 percent) of 356 applicable security controls for the CTC Update Portal and the SADI system. Privacy, Governmental Liaison, and Disclosure (PGLD) worked extensively with the SADI developers as it was developed and deployed to ensure the privacy aspects of the system were reviewed and implemented properly. Additionally, starting July 2021, PGLD implemented a collaborative effort with Cybersecurity to assess privacy specific controls at the system level via the system's annual security controls assessments. We

have clarified and strengthened internal processes regarding concurrence to operate in the production environment to further reduce risk to our operating environment.

Our goal is to ensure that taxpayers can access the online IRS services they need securely at any time of day.

In response to your recommendations, we have attached a corrective action plan to address the findings related to this audit.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at 202-317-5000, or a member of your staff may contact Gregory Zurmuhlen, IT, Director, Enterprise Program Controls, at 240-613-4257.

Attachment

Attachment

Audit #202120722, The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed

Recommendations

Recommendation 1: The Chief Information Officer should ensure that the ELC coaches comply with existing agency requirements related to the independent verification and validation of all ELC artifacts.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The recommendation is a part of the ELC Process; however, this was an internal error that will be addressed going forward ensuring we stay compliant, following process and procedure for the ELC Process as outlined in the IRM.

To remediate the recommendation, ELC has captured this error as a Lessons Learned and ELC Coaches have been briefed on their roles & responsibilities to comply with ELC standard requirements.

The MRR Procedure is located on the ELC Website.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy & Planning

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendation 2: The Chief Information Officer should ensure that only authorized approving authorities provide status updates and grant final approval of ELC artifacts during required milestone reviews.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The recommendation is a part of the ELC Process; however, this was an internal error that will be addressed going forward ensuring we stay compliant, following process and procedure for the ELC Process as outlined in the IRM.

To remediate the recommendation, ELC has implemented a detailed *ELC Required Artifacts Process Owner Approver Listing* and have briefed ELC Coaches on their role to comply with ELC standard requirements.

The *ELC Required Artifacts Process Owner Approver Listing* is located on the ELC Website.

2

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy & Planning

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendation 3: The Chief Information Officer should establish a formal process, which includes routine updates, to identify primary and proxy approvers for all ELC artifacts.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The recommendation is a part of the ELC Process; however, this was an internal error that will be addressed going forward ensuring we stay compliant, following process and procedure for the ELC Process as outlined in the IRM.

To remediate the recommendation, ELC has implemented a *Process Owner Meetings SOP* and a detailed *ELC Required Artifacts Process Owner Approver Listing* and briefed ELC Coaches on their role to comply with ELC standard requirements.

The *Process Owner (PO) Meetings SOP* is located on the ELC Coaches SharePoint site and the *ELC Required Artifacts Process Owner Approver Listing* is located on the ELC Website.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy & Planning

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendation 4: The Chief Information Officer should ensure that systems supported by CSPs have an approved IRS ATO prior to a system's deployment.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS has a robust documented ATO process in place, yet for this instance a onetime user error occurred which is not normal process. We will continue to follow our process and ensure we have quality assurance over the processes being followed.

3

IMPLEMENTATION DATE: N/A

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

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendation 5: The Chief Privacy Officer should establish a process that complies with Office of Management and Budget requirements regarding the selection, implementation, assessment, and continuous monitoring of privacy controls.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We have implemented this recommendation. The Privacy Compliance and Assurance operation in PGLD has established a process that is integrated with the IRS Cybersecurity assessments of the NIST controls. This process provides for the selection, implementation, assessment, and continuous monitoring of privacy controls.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): Chief Privacy Officer, Director Privacy Policy and Compliance

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendation 6: The Chief Privacy Officer should ensure that formal documentation is created that shows that all the privacy controls applicable to the Secure Access Digital Identity (SADI) system are properly selected, implemented, and assessed.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We will ensure that formal documentation is created that shows that all the privacy controls applicable to the SADI system are properly selected, implemented and assessed.

IMPLEMENTATION DATE: December 15, 2022

RESPONSIBLE OFFICIAL(S): Chief Privacy Officer, Director Privacy Policy and Compliance

CORRECTIVE ACTION MONITORING PLAN

4

We will monitor this corrective action as part of our internal management control system.

Recommendation 7: The Chief Information Officer should ensure that the Cybersecurity function validates that all required NIST physical and environmental protection and media protection controls are implemented.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. IRS will validate all required NIST physical and environmental and media protection controls are documented and assessed to reflect implementation status.

IMPLEMENTATION DATE: February 15, 2023

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

---

Recommendation 8: The Chief Information Officer should ensure the IRS prioritizes completing the processes that will validate newly built servers being placed into the production environment meet minimum compliance requirements and initiate vulnerability scanning and remediation during the server build process.

CORRECTIVE ACTION #1: IRS agrees with this recommendation. IRS will implement the process that will validate newly built servers being placed into the production environment meet minimum compliance requirements and initiate vulnerability scanning and remediation during the server build process.

IMPLEMENTATION DATE: September 15, 2022

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

---

Recommendation 9: The Chief Information Officer should ensure that all CTC Update Portal and SADI system associated POA&Ms (listed in Appendix II) are completed timely based on IRS-defined timelines and processes.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The CTCUP POA&Ms have been completed.

IMPLEMENTATION DATE: N/A

CORRECTIVE ACTION MONITORING PLAN

5

We will monitor this corrective action as part of our internal management control system.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The SADI application level POA&Ms (listed in Appendix II) will be completed timely based on IRS-defined timelines and processes.

IMPLEMENTATION DATE: December 12, 2022

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The program level POA&Ms (listed in Appendix II) will be completed timely based on IRS-defined timelines and processes.

IMPLEMENTATION DATE: December 12, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity with support from Applications Development and Enterprise IT Program Management Office.

Recommendation 10: The Chief Information Officer should prioritize remediation efforts on the two noncompliant SADI servers that have weighted noncompliance scores of less than 90 percent

CORRECTIVE ACTION #1: IRS agrees with this recommendation. IRS will prioritize remediation efforts on the two noncompliant SADI servers that have weighted noncompliance scores. An analysis of the servers indicates an upgrade is required and will involve SADI project team testing, validation, and production release time.

IMPLEMENTATION DATE: October 15, 2022

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

Appendix V

Glossary of Terms

Term	Definition
Artifact	The tangible result (output) of an activity or task performed by a project during the life cycle.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization to Operate	The management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorizing Official	A senior organizational 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	An entity offering cloud-based platform, infrastructure, application, or storage services.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. It attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or functionality of the information system.
Cryptography (Cryptographic)	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Event-Driven Security Controls Assessment	Initiated when changes are made to an information system that impact security controls. This process only applies to Federal Information Security Modernization Act reportable information systems with an existing security authorization. It does not apply to new systems without a security authorization.
Exploit	Any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.

Term	Definition
Federal Information Processing Standards Publication 199	Standards for categorizing information and information systems; establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems.
Federal Information Processing Standards Publication 200	Defines minimum security requirements for Federal information and information systems in 17 security-related areas.
Federal Information Security Modernization Act of 2014	Amendment to the Federal Information Security Management Act of 2002 that allows for further reform to Federal information security, signed 12 years after the passing of the original law. This bill amends Chapter 35 of Title 44 of the United States Code. The original statute (Federal Information Security Management Act of 2002) requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget.
Federal Risk and Authorization Management Program	A Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
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.
Go Live	To begin operating or to become available for use.
Identity Proofing	Verifying the claimed identity of an applicant by collecting and validating sufficient information, *e.g.,* identity history, credentials, and documents, about a person.
Information System Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Moderate-Impact System	An information system in which at least one security objective, *i.e.*, confidentiality, integrity, or availability, is assigned a Federal Information Processing Standards potential impact value of moderate and no security objective is assigned a potential impact value of high.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Ping	A signal sent to a host that requests a response to check if the host is available.

Term	Definition
Ping Monitoring	The practice of periodically pinging a computer or device and then sending alerts if a ping response is not received.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Production Environment	The location where the real-time staging of programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Program Level Plan of Action and Milestones	A tool that identifies required tasks to fix a weakness associated with findings that affect multiple IRS systems and organizations.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or NIST guidelines, whether related to a technical, operational, or management control.
Security Assessment and Authorization	The methodology by which an organization establishes and then demonstrates a sound information security posture for a specific system.
Security Assessment Report	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Tailoring	Modification of a standard approach to customize it for a specific situation. For example, ELC tailoring is modification of the standard ELC for the unique needs of a specific project.
Vulnerability	A weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.

Appendix VI

Abbreviations

ATO	Authorization to Operate
CSP	Cloud Service Provider
CTC	Child Tax Credit
ELC	Enterprise Life Cycle
FedRAMP	Federal Risk and Authorization Management Program
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SADI	Secure Access Digital Identity
SRM	Security Risk Management
TIGTA	Treasury Inspector General for Tax Administration

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.