TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed

July 23, 2024

Report Number: 2024-200-032

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

HIGHLIGHTS: Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed

Final Audit Report issued on July 23, 2024 **Report Number 2024-200-032**

Why TIGTA Did This Audit

In December 2015, Congress passed the *Federal Cybersecurity Requirements* legislation requiring the head of each agency to implement a single sign-on trusted identity platform, as developed by the General Services Administration, for individuals accessing each public website that requires user authentication. In December 2022, the IRS deployed Login.gov as one of its credential service providers (CSP) to offer authentication services.

This audit was initiated to evaluate the effectiveness and security of the Login.gov deployment.

Impact on Tax Administration

Login.gov must be a trusted identity platform that meets Federal and agency information security and investigative requirements. If these requirements are not met, identity proofing and authentications are weakened, potentially placing Personally Identifiable Information at risk of loss or theft, and investigations are jeopardized. In addition, if Federal Risk and Authorization Management Program continuous monitoring security reviews are not completed timely and reported consistently, the IRS would be unable to adequately and timely assess whether Login.gov's security controls are operating as intended, remain effective, and protect against threats and vulnerabilities.

What TIGTA Found

The IRS took steps to help move Login.gov towards complying with Federal security standards. For example, the IRS issued a document specifying the service offerings, requirements, and commitments that Login.gov must meet before expanding authentication services to IRS Identity Assurance Level (IAL) 2 applications.

However, additional security controls need improvement. The IRS does not have consolidated guidance, but rather various policies and related documents requiring CSPs to capture audit trail requirements for IAL2 applications. In addition, the policies and related documents do not include all audit trail, including investigative, data elements. Further, the Digital Identity Acceptance Statements (DIAS) for two IAL1 applications incorrectly included IAL2 security controls.

Continuous monitoring security reviews need improvement. The November 2022 through September 2023 continuous monitoring security reviews for Login.gov were not completed timely and/or the *Continuous Monitoring Reports* were not sent consistently to the Authorizing Official, resulting in the IRS not knowing that the Personally Identifiable Information for 57,417 IRS user authentications may have been sent to unauthorized locations outside of the United States. Further, none of the *Continuous Monitoring Reports* provide report elements, such as the name of the preparer and Authorizing Official, and the date the report was prepared, received, and reviewed to document security reviews.

What TIGTA Recommended

TIGTA made six recommendations to the Chief Information Officer. They included developing and periodically updating consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, that CSPs must capture and provide for IRS IAL2 applications; ensuring that guidance is updated to include a quality review process to help ensure DIASs are accurate; and ensuring that appropriate IRS management work in conjunction with Login.gov management to assess the extent and impact that the critical vulnerability had on IRS users who authenticated via Login.gov and may have had their Personally Identifiable Information sent to unauthorized locations outside of the United States.

The IRS agreed with all six recommendations and plans to periodically update consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, and ensure that IRS management work in conjunction with Login.gov management to assess the extent and impact of the unauthorized disclosure of Personally Identifiable Information. In addition, the IRS stated that it has developed consolidated guidance to comprise all audit trail data elements, including investigative elements; updated guidance to include a quality review process to help ensure that DIASs are accurate; and quality reviewed five DIASs.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

July 23, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

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

SUBJECT: Final Audit Report – Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed (Audit No.: 2024200022)

This report presents the results of our review to evaluate the effectiveness and security of the Login.gov deployment. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Information Technology Modernization*.

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

Table of Contents

Background

In December 2015, Congress passed the *Federal Cybersecurity Requirements* legislation, which requires the head of each agency to "implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services [also known as the General Services Administration (GSA)] in collaboration with the Secretary [of Commerce]."[1] Subsequently, the GSA developed, and in April 2017 launched, Login.gov to provide authentication and identity proofing services for Federal Government information systems and applications. Login.gov allows individuals to use a single username and password, *e.g.*, single sign-on, to access public services offered by other participating Federal Government agencies.[2]

The legislation also requires that Login.gov be a trusted identity platform that does not alter the authority of the Director of the National Institute of Standards and Technology (NIST), nor should it affect NIST standards process or discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security. In addition, because Login.gov is a Federal information system, its system standards must include minimum information security requirements as determined by the NIST Act of 2017.[3]

In December 2022, the Internal Revenue Service (IRS) deployed Login.gov to provide authentication services as one of its credential service providers (CSP). CSPs are independent and trusted third parties that issue user authenticators and provide electronic credentials for accessing an information system or application. The IRS leverages Login.gov as a CSP for its Secure Access Digital Identity system. According to IRS documentation, the Secure Access Digital Identity system employs NIST's digital identity standards.[4] These standards cover identity proofing and authentication of users, *e.g.*, employees, contractors, and private individuals, who interact with Federal Government information systems or applications over open networks, such as the Internet.

In accordance with NIST, information systems and applications are assigned one of three Identity Assurance Levels (IAL) based on an assessed risk profile of the sensitivity of information, such as Social Security Numbers, and the potential harm caused if an attacker made a successful false claim of an identity to gain system access. The three IALs established by NIST and that are used to verify users before granting system access to sensitive information are:

- IAL1: No requirement to link the applicant to a specific real-life identity. Authentication process attributes are self-asserted.
- IAL2: Evidence supports claimed identity and verifies applicant remotely or physically. Attributes can be asserted by CSPs to relying parties.

[1] 6 U.S.C. § 1523 (2015). See Appendix V for a glossary of terms.

[2] Examples of public services offered by other Federal Government agencies that use Login.gov include USAJOBS by the Office of Personnel Management and the Trusted Traveler Program by the Department of Homeland Security.

[3] 40 U.S.C. § 11331. Pub. L. No. 116-207.

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

- IAL3: Physical presence is required for identity proofing. Attributes must be verified by an authorized and trained CSP representative.

The IRS determines and assigns IALs for information systems and applications through the Digital Identity Risk Assessment (DIRA) process. IALs are also used to identify a CSP's secure credentialing capabilities and compliance with NIST identity proofing and authentication standards. For example, a CSP with a NIST IAL1 certification may not verify the identity of users accessing IAL2 applications. For IAL1 applications, users self-assert their identities. As of April 1, 2024, the IRS uses Login.gov to provide authentication services for two IAL1 applications: 1) Form 990-N Electronic Filing System (e-Postcard) and 2) Foreign Account Tax Compliance Act-Qualified Intermediary (FATCA-QI).[5]

In September 2023, the Treasury Inspector General for Tax Administration (TIGTA) issued a memorandum to the IRS regarding its efforts for the planned implementation of Login.gov's identity verification service.[6] TIGTA concluded that documented key events supported that at multiple stages, IRS management raised concerns regarding the implementation of Login.gov. According to IRS management, with emphasis towards Login.gov deployment provided by the Department of the Treasury, the IRS continued planning efforts and expending resources, *e.g.*, personnel and funds, to evaluate implementing Login.gov for IRS IAL2 applications even though Login.gov security concerns raised by IRS leadership and TIGTA's Office of Investigations were not fully addressed by the GSA.

Results of Review

Steps Have Been Taken to Help Move Login.gov Towards Complying With Federal Security Standards

Within the Information Technology organization's Cybersecurity function, the Security Risk Management organization timely completed the initial analysis of Login.gov's Federal Risk and Authorization Management Program (FedRAMP) security package.[7] The results were reviewed and accepted by the Authorizing Official for Login.gov prior to its deployment. This acceptance was made with the understanding that system flaws would be monitored and mitigated at the appropriate time.

The Privacy and Civil Liberties Impact Assessment for the Secure Access Digital Identity system, which includes Login.gov, was updated and publicly posted to the IRS website. The privacy assessment is a process that analyzes how Sensitive But Unclassified data, including Personally

[5] Pub. L. No. 111-147, Subtitle A, 124 Stat 97 (codified in scattered sections of 26 U.S.C.). Users can also authenticate using a second CSP that offers both IAL1 and IAL2 certifications.

[6] TIGTA, Report No. 2023-2S-070, *Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification* (Sept. 2023).

[7] Examples of artifacts in the FedRAMP security package for Login.gov include: the Plans of Action and Milestones, the Digital Identity Acceptance Statement, and the Information System Contingency Plan.

Identifiable Information and tax information, are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed. Further, Login.gov's capacity of user identity verification attempts per second was confirmed to meet IRS requirements.

In September 2023, the IRS issued its *Login.gov IAL2 SADI [Secure Access Digital Identity system] Integration Consideration for Filing Season 2024* (hereafter referred to as the *Login.gov Integration Consideration* document) to the Department of the Treasury. The *Login.gov Integration Consideration* document specifies the service offerings, requirements, and commitments that Login.gov must meet prior to expanding authentication services to IRS IAL2 applications. Specifically, it states that Login.gov must:

- Meet NIST IAL2 and Authorization Assurance Level 2 standards, including liveness presentation attack detection.
- Obtain independent certification of alignment to NIST, Special Publication 800-63 Revision 3, assurance levels.
- Complete and execute a memorandum of understanding to share fraud data subject to IRS Publication 1075.[8]
- Implement four specific controls to improve its anti-fraud program as required by the Office of Management and Budget. Login.gov should:
    - Rely on the analysis of identity evidence for its anti-fraud controls. Registration data, including unsuccessful registration attempts data, should be actively monitored for high-risk activity by a dedicated anti-fraud program.
    - Establish a retention period and a set of retained data elements from identity evidence and other sources that are based on a risk management process designed to balance privacy, customer experience, and security interests, consistent with applicable law, and considering technical privacy-preserving measures that could still enable anti-fraud analysis where feasible.
    - Implement fraud performance metrics that measure overall fraud rates in identity verification and authentication, which may require additional anti-fraud controls or mechanisms that attempt to analyze the overall fraud rate.
    - Continue to mature its fraud program capabilities, including governance and monitoring and detection capabilities as a core program priority.
- Address all gaps identified by the IRS during the fraud tabletop exercise. For example, gaps include:
    - Providing a list of identified fraud types.
    - Delivering a playbook that details step-by-step actions that will be executed when handling fraudulent attempts.
    - Developing a process for sharing specific fraudulent attempts with the IRS and TIGTA.

[8] IRS, Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information* (Nov. 2021).

  - Providing procedures for managing single and multiple suspected fraudulent accounts.
- Ensure that only one active IAL2 credential is permitted per unique user. The unique user must have profile capability to view and manage their Login.gov account entitlements and activities, including website visits and device locations.
- Operate a customer support center serving all Login.gov end users.

The IRS also requested that the Department of the Treasury disseminate the *Login.gov Integration Consideration* document to the GSA.[9]

In November 2023, we asked the IRS to provide a status update on their *Login.gov Integration Consideration* document. According to written internal correspondence between the IRS Acting Chief Information Officer; Chief Privacy Officer; Director, Identity Assurance; and the Authorizing Official for Login.gov, dated November 13, 2023, the IRS does not know whether the Department of the Treasury sent the *Login.gov Integration Consideration* document to the GSA, nor do they know whether the GSA has sufficiently addressed and met the requirements. On December 5, 2023, the IRS provided the following statement to TIGTA:

> *The timeframe for considering Login.gov integration at IAL2 for Filing Season 2024 has passed. The IRS will continue to use our current CSP providing IAL2 services and conduct market research to identify additional CSP options that meet IAL2 [security] standards and IRS requirements. [The Department of the] Treasury is the lead of this initiative. When [the] GSA [(Login.gov)] notifies [the Department of the] Treasury that they can meet IRS requirements, [the Department of the] Treasury will notify [the] IRS on when to resume IAL2 integration activities.*

Taking these steps will help move the IRS towards ensuring that Login.gov is NIST IAL2 compliant and reduce the risk of unauthorized accesses going undetected. However, we identified additional security controls that need improvements.

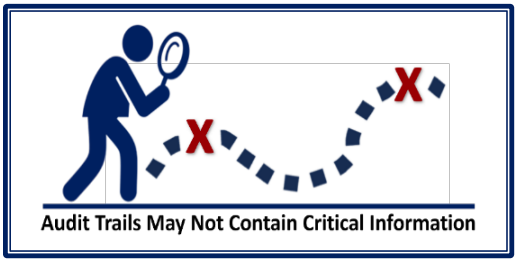
Requirements for Credential Service Providers to Capture and Provide Sufficient Audit Log Content Need Improvement

TIGTA's Office of Investigations and the IRS's Criminal Investigation analyze audit logs from information systems and applications to pursue, investigate, and mitigate emerging threats to the IRS's ability to perform Federal tax administration. TIGTA's Office of Investigations issued its *TIGTA Audit Trail Needs for the Secure Access Digital Identity Project* (hereafter referred to as the *Audit Trail Needs* document) to the IRS on three different occasions, *i.e.*, December 2020, March 2021, and June 2022, and on multiple occasions requested that the IRS require CSPs, *e.g.*, Login.gov, capture and provide specific audit trail requirements for IAL2 applications. The *Audit Trail Needs* document lists specific audit trail requirements and details the necessary data elements that CSP audit trails for IAL2 applications must include for investigations to be conducted properly. However, our review of the IRS's *Login.gov Integration Consideration*

[9] The IRS is leveraging a contract between the Department of the Treasury and Login.gov for authentication services. As a result, the IRS relies on the Department of the Treasury to convey its requirements to Login.gov.

document determined it does not specify that Login.gov must comply with and meet the audit trail requirements in the *Audit Trail Needs* document.

The IRS does not have consolidated guidance requiring CSPs that leverage the Secure Access Digital Identity system to capture all audit trail, including investigative, data elements. The *Login.gov Integration Consideration* document states that prior to providing identity proofing services for IAL2 applications, Login.gov must meet the draft *Treasury/IRS/Login.gov Shared Requirements* (also known as the IRS CSP baseline requirements but applies to Login.gov only). However, TIGTA's Office of Investigations review of IRS CSP baseline requirements determined that they omit critical investigative audit trail data elements listed in its *Audit Trail Needs* document. For example, missing investigative audit trail data elements include:



[redacted]

Instead, Cybersecurity function management stated that they rely on several policies and related documents to capture all audit trail, including investigative, data elements that CSPs are required to capture and provide for IAL2 applications. Examples include:

- Internal Revenue Manual, 10.8.63, *Information Technology (IT) Security, Central Log Server Security Policy*.
- *Generalized CSP NIST – Based Data Element Requirements Version 3.0*.
- Draft *Treasury/IRS/Login.gov Shared Requirements*.
- *IRS External Identity Federation Trust Framework*.

However, TIGTA's Office of Investigations performed a crosswalk analysis of the policies and related documents to its *Audit Trail Needs* document and determined that they do not include all investigative audit trail data elements necessary for investigations to be conducted properly.

According to the Government Accountability Office's standards, "Management holds service organizations [*e.g.*, CSPs] accountable for their assigned internal control responsibilities.[10] Management communicates to the service organization the objectives of the entity and their related risks…and the expectations of competence for its role that will enable the service organization to perform its internal control responsibilities." It also states that management improves the effectiveness and efficiency of its program operation by linking the objectives of

[10] Government Accountability Office (GAO), GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

the entity to its mission. In addition, the Internal Revenue Manual states that IRS management must ensure that investigations are not jeopardized.[11]

During initial discussions with Cybersecurity function management on whether Login.gov and all CSPs are required to capture and provide complete audit trail requirements, management maintained that their analyses of the various policies and related documents included all required audit trail, including investigative, data elements. However, after repeated requests by TIGTA, management agreed to perform another analysis of their policies and related documents and determined that some investigative audit trail data elements are not included. IRS management stated that they have not developed consolidated guidance, which includes all audit trail data elements because:

- Audit trails are constantly evolving due to information technology changes. Each CSP has different processes and methods for storing data.
- "It is beyond the scope of [their] program to determine, define, or otherwise document guidance for evidence gathering purposes."

However, the *Audit Trail Needs* document has remained the same since it was first issued to the IRS in December 2020. In addition, requests by TIGTA's Office of Investigations for the IRS to ensure that CSPs include the *Audit Trail Needs* document data elements to facilitate investigative case work and the betterment of our Nation's tax system is in keeping with the IRS's and TIGTA Office of Investigations' missions.

As a result of this review, in March 2024, Cybersecurity function management updated its *Generalized CSP NIST – Based Data Element Requirements Version 4.3* to include the investigative audit trail data elements listed in the TIGTA Office of Investigations' *Audit Trail Needs* document. However, an analysis of the updated *Generalized CSP NIST – Based Data Element Requirements Version 4.3* document showed it was still missing important audit trail data elements from the *Treasury/IRS/Login.gov Shared Requirements*.

According to Applications Development function personnel, the IRS is participating in the Department of the Treasury's market research to identify additional CSPs that will provide identity proofing services for IAL2 applications. It is critical that the IRS requires CSPs, including Login.gov, to capture and provide all audit trail, including investigative, data elements identified in the IRS's policies and related documents as well as in the TIGTA Office of Investigations' *Audit Trail Needs* document. It is also important to have consolidated guidance to ensure the efficient and effective identification and implementation of CSP requirements. This will reduce the risk of Login.gov and future CSPs omitting critical investigative audit trail data elements and potentially jeopardize investigations.

[11] Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 2023).

The Chief Information Officer should:

Recommendation 1: Develop and periodically update consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, that CSPs must capture and provide for IRS IAL2 applications.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer has taken appropriate action to develop and will periodically update consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations. TIGTA investigation requirements have been incorporated in the CSP Data Elements Requirements document.

Recommendation 2: Ensure that a process is in place to validate that all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, are being captured and can be provided by Login.gov prior to using its identity proofing services for IRS IAL2 applications.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure that a process is in place to validate that all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, are being captured.

Digital Identity Acceptance Statements Contain Inaccurate Information

The DIRA process and assessment help ensure that public-facing web applications comply with the assigned assurance type, *e.g.*, IAL, Authenticator Assurance Level, and Federation Assurance Level, and assurance level throughout an application's life cycle. The results of the assessment and subsequent reassessments, along with any required identity proofing and authentication security controls, are documented in a Digital Identity Acceptance Statement (DIAS). Our review of the DIASs for the two IAL1 applications, *i.e.*, e-Postcard and FATCA-QI, included IAL2 security controls not applicable to the applications.

The Security Risk Management organization incorrectly added IAL2 security controls to the DIASs for e-Postcard and FATCA-QI in September and October 2022, respectively. The IAL2 security controls were added because of a reassessment of the IAL1 applications when the Secure Access Digital Identity system was launched and a second CSP started offering identity proofing and authentication services. On February 14, 2024, two days after being notified, the Security Risk Management organization provided TIGTA updated DIASs by deleting the IAL2 security controls. However, our review of the updated DIASs identified new errors: the deletions were not properly recorded in the document change tracker and the FATCA-QI DIAS contained e-Postcard information.

IRS standard operating procedure states that the DIRA process must follow risk assessment guidelines from NIST and determine the appropriate assurance type and level for a given application.[12] In addition, the standard operating procedure includes three main components as

[12] IRS, *IRS Digital Identity Risk Assessment (DIRA) Standard Operating Procedure* (Aug. 2021).

part of the DIRA process: 1) assess the assurance level, 2) assign an assurance level for implementation, and 3) approve the DIAS and provide oversight. The standard operating procedure also states that reassessments should be performed annually or when an event-based trigger, *e.g.*, DIRA process, transaction data, or risk environment change, occurs to ensure that the data and information in the DIAS are up to date.

According to management from the Security Risk Management organization, due to limited resources, they copied and pasted "IAL2 template language" into the FATCA-QI and e-Postcard DIASs and did not perform a quality review prior to issuance.

A successful DIRA process uses a comprehensive approach to accurately document the life cycle of digital identity assessments and digital transactions. If an application's DIAS contains inaccurate information, assurance levels could be implemented incorrectly or insufficiently. This could lead to weak user identity proofing and authentication and potentially place Personally Identifiable Information at risk of loss or theft.

Recommendation 3: The Chief Information Officer should ensure that DIRA guidance is updated to include a quality review process to help ensure that DIASs are accurate prior to issuance.

Management's Response: The IRS agreed with this recommendation. DIRA guidance has been updated to include a quality review process to help ensure that DIASs are accurate prior to issuance. The quality review process has been performed on five DIASs.

Office of Audit Comment: While the IRS updated the DIRA guidance to include a quality review process, it was updated subsequent to the Security Risk Management organization providing the revised DIASs for e-Postcard and FATCA-QA. Both DIASs still contained errors.

Continuous Monitoring Security Reviews Need Improvement

Login.gov continuous monitoring security reviews were not completed timely and/or sent consistently to the Authorizing Official for review

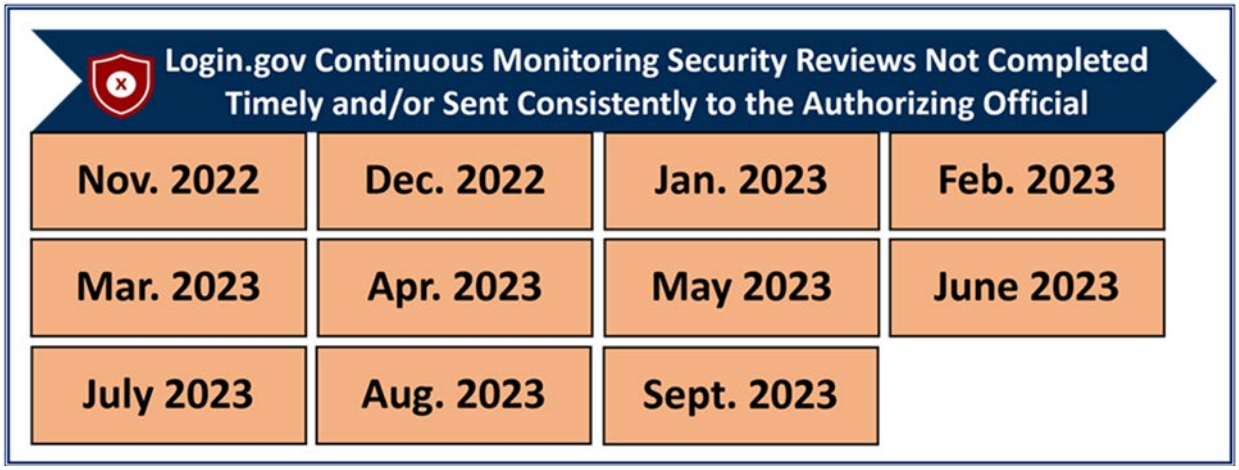
The Authorizing Official signed and issued the Authorization to Operate for Login.gov in November 2022, which is when the IRS's monthly FedRAMP continuous monitoring security reviews should have begun. However, in early February 2023, we found that the Security Risk Management organization had not yet obtained access to the FedRAMP repository for Login.gov so that the [redacted] could begin the continuous monitoring security reviews. After we brought this matter to the IRS's attention, management from the Security Risk Management organization stated that they would obtain access to the FedRAMP repository, and the [redacted] would start retroactively completing the continuous monitoring security reviews and documenting the results in a *Continuous Monitoring Report* for each of the months missed.

While the [redacted] started retroactively completing the continuous monitoring security reviews, the results were not sent consistently to the Authorizing Official for

review. Specifically, it was not until early June 2023, nearly seven months after the Authorization to Operate for Login.gov was issued, approximately six months after the IRS deployed Login.gov in December 2022, and nearly four months after TIGTA brought it to the IRS's attention that the *Continuous Monitoring Reports* from November 2022 through April 2023 were completed and sent to the Authorizing Official.[13] We also found that the May 2023 *Continuous Monitoring Report* was not completed and sent timely to the Authorizing Official until July 2023.

In November 2023, we followed up with the Security Risk Management organization and determined that while the [redacted] performed continuous monitoring security reviews for June through September 2023, the *Continuous Monitoring Reports* were not sent to the Authorizing Official for review as required.[14] The [redacted] responded to our follow up and sent the missing reports to the Authorizing Official. Figure 1 shows the months that FedRAMP continuous monitoring security reviews were not completed timely and/or the results were not sent consistently to the Authorizing Official.

Figure 1: Months FedRAMP Continuous Monitoring Security Reviews Were Not Completed Timely and/or Sent Consistently to the Authorizing Official



Source: TIGTA's analysis of FedRAMP continuous monitoring security reviews for Login.gov.

From November 2022 through September 2023, when continuous monitoring security reviews were not completed timely and sent consistently to the Authorizing Official for review, 613,407 IRS user authentications occurred.[15]

- 601,506 IRS user authentications for the e-Postcard application.
- 11,901 IRS user authentications for the FATCA-QI application.

During the months when continuous monitoring security reviews were not completed timely, *i.e.*, November 2022 through May 2023, our review of the *Continuous Monitoring Reports* identified a critical vulnerability. The January 2023 *Continuous Monitoring Report* stated that

[13] See Appendix III for the continuous monitoring security review timeline of select events.

[14] Due to the timing of our follow-up, the October 2023 *Continuous Monitoring Report* had not yet been completed.

[15] The number of authentications includes users who authenticated and signed into their accounts multiple times. Users, including repeat users, are exposed to potential security vulnerabilities each time they authenticate and log into the IAL1 applications when FedRAMP continuous monitoring security reviews are not completed and sent to the Authorizing Official for review.

since Login.gov's deployment, Personally Identifiable Information is being sent to unauthorized locations outside of the United States by a Login.gov vendor's fraud prevention solution. Because the [redacted] did not timely complete the monthly continuous monitoring security reviews and consistently send the *Continuous Monitoring Reports*, the Authorizing Official was not made aware of this critical vulnerability until June 2023 to assess whether the cloud service's security posture remains sufficient for the IRS's use or whether a risk-based decision was necessary. In addition, subsequent *Continuous Monitoring Reports* provided additional updates on the vulnerability as follows:

- February 2023 – Login.gov's vendor reconfigured its fraud prevention solution to locations within the United States.
- April 2023 – The vendor's fraud prevention solution was still not operational and pending validation and compliance with Login.gov's policy.

Continuous Monitoring Reports through September 2023 did not provide further updates on the vulnerability.

In April 2024, Login.gov management stated that, "IRS users have never used Login.gov for IAL2 [(identity verification)] services, and therefore were not impacted by [sic] [the critical vulnerability]." We requested and Login.gov management provided the source code and configuration settings for both its authentication and identity verification services as evidence that its vendor's fraud prevention solution affected only users of their identity verification service.[16] We reviewed the documentation provided but were unable to conclusively confirm that Personally Identifiable Information associated with the 57,417 IRS user authentications were not affected by the critical vulnerability.[17]

In May 2024, Login.gov management stated that:

> *…some Login.gov accounts may have had their information sent to [sic] [Login.gov vendor's fraud prevention solution] during the identity proofing process when accessing an app[lication] from another agency that required IDV [identity verification service]. Meanwhile, that same user may have also used IRS [applications] at the IAL1 level.*

According to Publication 1075, to use a cloud service to receive, process, store, access, protect, and/or transmit Federal Tax Information, an agency must leverage vendors and services where 1) all Federal Tax Information physically resides in systems located within the United States and 2) all accesses and support of the systems and services are performed from the United States, its possessions, and Territories. In addition, the IRS cloud continuous monitoring strategy states that FedRAMP continuous monitoring security reviews must begin once an Authorization to Operate has been issued for an application that is leveraging a FedRAMP authorized cloud service.[18]

[16] Login.gov's authentication service is self-asserted and requires that users create a secure account using an e-mail address, password, and multifactor authentication. For its identity verification service, users first complete the authentication service requirements, and then verify their identity using additional documentation.

[17] The 57,417 IRS user authentications are the number of authentications that occurred from December 4, 2022, when the IRS deployed Login.gov to February 16, 2023, at 4:35 PM Eastern Standard Time, when the vulnerability was remediated.

[18] IRS, *IRS Cloud Continuous Monitoring Strategy* (Sept. 2022).

On a monthly basis, an assigned [redacted] must review the cloud service's continuous monitoring artifacts that are maintained on a private FedRAMP repository. The [redacted] must collect and review various predefined continuous monitoring metric data and document their analysis in a monthly *Continuous Monitoring Report*.[19] The [redacted] is also required to send the monthly *Continuous Monitoring Reports* to the applicable Authorizing Official in order for the official, along with Cybersecurity function subject matter experts, to ensure that the cloud service's security posture remains sufficient for the agency's use of the system and to make knowledgeable, risk-based decisions on the cloud service.

Management from the Security Risk Management organization explained that because of human error, they did not submit the Authorization to Operate for Login.gov to FedRAMP. This error interrupted the prompt for the IRS to obtain access to the FedRAMP repository for Login.gov and start the continuous monitoring security reviews. Management also explained that they did not send the *Continuous Monitoring Reports* to the Authorizing Official from June through September 2023 due to an "oversight."

A successful continuous monitoring security program generates actionable data for review that can be used to make timely risk management decisions. Because the IRS did not always complete the required Login.gov continuous monitoring security reviews timely and did not send the *Continuous Monitoring Reports* consistently to the Authorizing Official for review, the IRS was unable to adequately and timely assess whether Login.gov's security controls were operating as intended, remained effective, and protected against threats and vulnerabilities. As a result, user data associated with the 613,407 IRS user authentications for Login.gov were potentially placed at risk.

The Chief Information Officer should ensure that:

Recommendation 4: Current continuous monitoring security review guidelines are followed by timely performing reviews of Login.gov artifacts, documenting the results in a monthly *Continuous Monitoring Report*, and timely submitting the report to the Authorizing Official for review as required.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure that the current continuous monitoring security review guidelines are followed by performing timely reviews of Login.gov artifacts, documenting the results in a monthly *Continuous Monitoring Report*, and timely submitting the report to the Authorizing Official for review as required.

Recommendation 5: Appropriate IRS management works in conjunction with Login.gov management to assess the extent and impact that the critical vulnerability had on the users who authenticated via Login.gov to access IRS applications and may have had their Personally Identifiable Information sent to unauthorized locations outside of the United States.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure that IRS management works in conjunction with

[19] Examples of predefined continuous monitoring metric data include: the number of identified vulnerabilities, the average time to patch the vulnerabilities, the number of open and closed Plans of Action and Milestones, and the number and type of identified audit incidents.

Login.gov management to assess the extent and impact of the unauthorized disclosure of Personally Identifiable Information.

Login.gov *Continuous Monitoring Reports* lack essential report elements

Monthly *Continuous Monitoring Reports* describe and document the continuous monitoring security reviews performed by the [redacted]. The Authorizing Official must timely review the *Continuous Monitoring Reports* to assess the level of risk of applications operating on a cloud service, make informed decisions for ongoing authorizations to operate, and ensure that CSPs timely address or mitigate vulnerabilities identified. However, we found that from November 2022 to September 2023, the monthly Login.gov *Continuous Monitoring Reports* did not provide report elements, such as the name of the preparer and Authorizing Official, and the date the report was prepared, received, and reviewed to effectively document security reviews performed by the [redacted] and Authorizing Official.

According to the Government Accountability Office's standards, "Documentation is a necessary part of an effective internal control and is required for the effective design, implementation, and operating effectiveness of an entity's internal control system." It also states that "Management holds entity personnel accountable for performing their assigned internal control responsibilities. Management should also process data into quality information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis."

IRS policies and procedures do not require nor does the *Continuous Monitoring Report Template* provide space for the elements to be included in the reports. If the *Continuous Monitoring Reports* do not include the report elements, stakeholders may not easily identify the preparer and Authorizing Official to discuss and address urgent security issues. In addition, documenting timelines would enable the IRS to preserve historical data for use in trend analyses and to make more informed and accurate risk management decisions that protect taxpayer data.

Recommendation 6: The Chief Information Officer should ensure that the FedRAMP continuous monitoring security review guidelines and report template are updated to ensure that the *Continuous Monitoring Reports* include essential report elements.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure that the FedRAMP continuous monitoring security review guidelines and report template are updated to include additional report elements to make informed and accurate risk management decisions.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness and security of the Login.gov deployment. To accomplish our objective, we:

- Determined whether the IRS's operational security controls were effective to ensure that the Login.gov's security posture was sufficient for deployment by reviewing information system security, DIRA, and identity proofing documentation for cloud services and CSPs as well as *Continuous Monitoring Reports*. We also interviewed Information Technology organization personnel.
- Determined whether the IRS's operational security controls ensured that GSA's Login.gov audit records, *e.g.*, audit logs and audit trails, met Federal, agency, and stakeholder requirements by reviewing Federal and IRS policies, procedures, and guidance, and audit trail documentation as well as interviewed Information Technology organization and TIGTA's Office of Investigations personnel.
- Evaluated the effectiveness of the Login.gov deployment by reviewing information system security, privacy, and transaction capacity documentation.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Applications Development and Cybersecurity functions located at the New Carrollton Federal Building in Lanham, Maryland, during the period October 2023 through April 2024. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the review were Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Catherine Sykes, Audit Manager; David Allen, Lead Auditor; Amin Sejtanic, Auditor; and Emily Bridges, Auditor.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Government Accountability Office's *Standards for Internal Control in the Federal Government*; NIST, Special Publication 800-63 Revision 3; and various Federal and IRS policies, procedures, and guidance related to information system deployment and security controls. We evaluated these controls by interviewing Information Technology organization and TIGTA's Office of Investigations personnel 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:

- Reliability of Information – Potential; one consolidated guidance document that did not require CSPs to capture and provide all audit trail, including investigative, data elements (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

The IRS does not have consolidated guidance requiring CSPs that leverage the Secure Access Digital Identity system to capture all audit trail, including investigative, data elements. The IRS's *Login.gov Integration Consideration* document does not specify that Login.gov must comply with and meet audit trail requirements for IAL2 applications in TIGTA Office of Investigations' *Audit Trail Needs* document. Instead, Cybersecurity function management stated that they rely on several policies and related documents to capture all audit trail, including investigative, data elements that CSPs are required to capture and provide for IAL2 applications. However, TIGTA's Office of Investigations performed a crosswalk analysis of the policies and related documents to its *Audit Trail Needs* document and determined that they do not include all investigative audit trail data elements necessary for investigations to be conducted properly.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; two DIASs contained incorrect information for two IAL1 applications (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

The Security Risk Management organization incorrectly added IAL2 security controls to the DIASs for the two IAL1 applications, *i.e.*, e-Postcard and FATCA-QI, in September and October 2022, respectively.[1] Two days after being notified, the Security Risk Management organization provided TIGTA updated DIASs by deleting the IAL2 security controls. However, our review of the updated DIASs identified new errors: the deletions were not properly recorded in the document change tracker and the FATCA-QI DIAS contained e-Postcard information.

[1] Pub. L. No. 111-147, Subtitle A, 124 Stat 97 (codified in scattered sections of 26 U.S.C.). Users can also authenticate using a second CSP that offers both IAL1 and IAL2 certifications.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 613,407 IRS user authentications from two IAL1 applications when monthly FedRAMP continuous monitoring security reviews were not completed timely and/or the results were not sent consistently to the Authorizing Official for review (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

The [redacted] did not complete timely the monthly FedRAMP continuous monitoring security reviews for Login.gov and/or send consistently the results to the Authorization Official for review from November 2022 through September 2023. There were 613,407 IRS user authentications [601,506 IRS user authentications for e-Postcard + 11,901 IRS user authentications for FATCA-QI] using Login.gov to access the two IAL1 applications.[2]

[2] The number of authentications includes users who authenticated and signed into their accounts multiple times. Users, including repeat users, are exposed to potential security vulnerabilities each time they authenticate and log into the IAL1 applications when FedRAMP continuous monitoring security reviews are not completed and sent to the Authorizing Official for review.

Appendix III

Timeline of Select Events for Login.gov Continuous Monitoring Security Reviews

Vulnerability information. Continuous security monitoring event. Information sent to Authorizing Official.

11/17/2022	Login.gov Authorization to Operate issued.
12/4/2022	Login.gov deploys for two IRS IAL1 applications.
1/26/2023	Vulnerability reported in Login.gov FedRAMP repository and shows that the Personally Identifiable Information was sent to unauthorized locations outside of the United States by a Login.gov vendor's fraud prevention solution during identity proofing.
2/14/2023	TIGTA determines that the IRS had not yet obtained access to the FedRAMP repository for Login.gov to begin the continuous monitoring security reviews.
2/15/2023	The Security Risk Management organization obtains first access to the Login.gov FedRAMP repository.
2/16/2023	Vendor of Login.gov responds to vulnerability and reconfigures its fraud prevention solution to locations within the United States.
4/30/2023	The Login.gov vendor's fraud prevention solution was still not operational and pending validation and compliance with Login.gov's policy.
6/5/2023	The November 2022 through April 2023 monthly *Continuous Monitoring Reports* are sent late to the Authorizing Official. The Authorizing Official receives late notification of the vulnerability.
7/2/2023	The May 2023 monthly *Continuous Monitoring Report* is sent late to the Authorizing Official.
12/14/2023	The June through September 2023 *Continuous Monitoring Reports* are sent late to the Authorizing Official.

Source: TIGTA's analysis of Login.gov select events for Fiscal Years 2022 and 2023.

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

June 17, 2024

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal, Chief Information Officer Kaschit D. Pandya Digitally signed by Kaschit D. Pandya Date: 2024.06.17 14:05:44 -04'00'

SUBJECT: Draft Audit Report – Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed (Audit #2024200022)

Thank you for the opportunity to review and comment on the draft audit report and address your observations. The auditors acknowledge that the IRS is taking steps to help move Login.gov towards complying with Federal security standards. Specifically, the IRS is actively working towards compliance in Identity Assurance Level (IAL) 2 applications with multi-agency stakeholders.

The IRS also recognizes the need for additional improvements to address security and monitoring controls and is committed to fully implementing and documenting all agreed upon corrective actions.

Information Technology security is of the utmost importance to the IRS mission. We agree with the Treasury Inspector General for Tax Administration's recommendations and have already begun to address deficiencies. Our corrective action plans for the six recommendations and three outcome measures are identified in the report.

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 Shelia Walker, Director of Identity Access Management, at (240) 613-3371.

Attachment

Attachment

TIGTA Audit 2024200022 - Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed

Recommendations

RECOMMENDATION 1: The Chief Information Officer should develop and periodically update consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, that CSPs must capture and provide for IRS IAL2 applications.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. The Chief Information Officer has taken appropriate action to develop and will periodically update consolidated guidance to comprise all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations. TIGTA investigation requirements have been incorporated in our CSP Data Elements Requirements document.

IMPLEMENTATION DATE: Implemented

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

RECOMMENDATION 2: The Chief Information Officer should ensure that a process is in place to validate that all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, are being captured and can be provided by Login.gov prior to using its identity proofing services for IRS IAL2 applications.

CORRECTIVE ACTION 2: The IRS agrees with the recommendation. The Chief Information Officer will ensure a process is in place to validate that all audit trail data elements, including investigative elements provided by TIGTA Office of Investigations, are being captured.

IMPLEMENTATION DATE: September 15, 2024

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

RECOMMENDATION 3: The Chief Information Officer should ensure that DIRA guidance is updated to include a quality review process to help ensure DIASs are accurate prior to issuance.

CORRECTIVE ACTION 3: The IRS agrees with the recommendation. The DIRA guidance has been updated to include a quality review process to help ensure DIASs are accurate prior to issuance. The quality review process has been performed on 5 DIASs.

Attachment

TIGTA Audit 2024200022 - Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed

MANAGEMENT ACTION 3: In response to this finding, the Cybersecurity organization updated the Digital Identity Risk Assessment (DIRA) Process Guide to include a quality review process for DIASs prior to issuance.

IMPLEMENTATION DATE: Implemented

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

RECOMMENDATION 4: The Chief Information Officer should ensure that current continuous monitoring security review guidelines are followed by timely performing reviews of Login.gov artifacts, documenting the results in a monthly Continuous Monitoring Report, and timely submitting the report to the Authorizing Official for review as required.

CORRECTIVE ACTION 4: The IRS agrees with the recommendation. The Chief Information Officer will ensure that the current continuous monitoring security review guidelines are followed by performing timely reviews of Login.gov artifacts, documenting the results in a monthly Continuous Monitoring Report, and timely submitting the report to the Authorizing Official for review as required.

IMPLEMENTATION DATE: November 15, 2024

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

RECOMMENDATION 5: The Chief Information Officer should ensure that appropriate IRS management work in conjunction with Login.gov management to assess the extent and impact that the critical vulnerability had on the users who authenticated via Login.gov to access IRS applications and may have had their Personally Identifiable Information sent to unauthorized locations outside of the United States.

CORRECTIVE ACTION 5: The IRS agrees with the recommendation. The Chief Information Officer will ensure IRS management works in conjunction with Login.gov management to assess the extent and impact of unauthorized disclosure of Personally Identifiable Information.

IMPLEMENTATION DATE: September 15, 2024

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

RECOMMENDATION 6: The Chief Information Officer should ensure that the FedRAMP continuous monitoring security review guidelines and report template are

Attachment

TIGTA Audit 2024200022 - Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed

updated to ensure that the Continuous Monitoring Reports include essential report elements.

CORRECTIVE ACTION 6: The IRS agrees with the recommendation. The Chief Information Officer will ensure that the FedRAMP continuous monitoring security review guidelines and report template are updated to include additional report elements to make informed and accurate risk management decisions.

IMPLEMENTATION DATE: November 15, 2024

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

Appendix V

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
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	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	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.
Chief Information Officer	Leads the IRS Information Technology organization and advises the IRS Commissioner about information technology matters, manages all IRS information system resources, and is responsible for delivering and maintaining modernized information systems throughout the IRS.
Cloud	The use of computing resources, *e.g.*, hardware and software, which are delivered as a service over a network (typically the Internet).
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
Cookie	A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.
Credential Service Provider	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.

Term	Definition
Electronic Filing System (e-Postcard)	A web-based application used for online submission of IRS Form 990-N for annual filings for small tax-exempt organizations with reporting revenue of $50,000 or less.
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.
Federal Tax Information	Includes any information created by the recipient that is derived from Federal return or return information received from the IRS or obtained through a secondary source. It may include Personally Identifiable Information, such as Social Security Number, taxpayer mailing address, and taxpayer e-mailing address.
Filing Season	The period from January 1 through mid-April when most individual income tax returns are filed.
Foreign Account Tax Compliance Act-Qualified Intermediary[1]	A secure web-based platform that enables users to apply, renew, or terminate an existing agreement and manage their information.
General Services Administration	An independent agency of the Federal Government, established to help manage and support the basic functioning of Federal agencies. It supplies products and services to U.S. Government offices, including real estate acquisition and facilities management.
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.
Internet Protocol Address	A unique code that identifies a computer network or a particular computer or other device on a network.
Login.gov	A service that offers secure and private online access to Federal Government programs, such as Federal benefits, services, and applications. With a Login.gov account, users can sign into multiple Federal Government websites with the same e-mail address and password.
Memorandum of Understanding	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
Multifactor Authentication	Verifying the identity of a user, process, or device using two or more factors to achieve authentication, often as a prerequisite to allowing access to resources in an information system. Factors include: 1) something you know, *e.g.*, password/Personal Identification Number; 2) something you have, *e.g.*, cryptographic identification device, token; or 3) something you are, *e.g.*, biometric.

[1] Pub. L. No. 111-147, Subtitle A, 124 Stat 97 (codified in scattered sections of 26 U.S.C.). Users can also authenticate using a second CSP that offers both IAL1 and IAL2 certifications.

Term	Definition
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Office of Management and Budget	Federal agency that oversees the preparation and administration of the Federal budget and coordinates Federal procurement, financial management, information, and regulatory policies.
Platform	A computer or hardware device, associated operating system, or virtual environment on which software can be installed or run.
Policy	A guiding principle, typically established by senior management, which is adopted by an organization to influence and determine decisions.
Publication 1075	Provides guidance to ensure that the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or subcontractors adequately protect the confidentiality of Federal Tax Information.
Requirement	Describes a condition or capability to which a system must conform, either derived directly from user needs, or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Secure Access Digital Identity System	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. It is a major system that delivers a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
Security Risk Management Organization	An office within the Cybersecurity function that provides guidance and direction to the IRS enterprise-wide disaster recovery efforts as well as a comprehensive, business-centric information technology service continuity management program designed to protect IRS operations, assets, and information.
Source Code	A set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler.
Tabletop Exercise	Brings members of the incidence response team together to simulate their response to a security and privacy incident scenario(s). It is a cost-effective and efficient way to identify gaps, overlaps, and discrepancies in the incidence response handling capabilities.
Timestamp	Digital record of the time of occurrence of a particular event.
Vulnerability	Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

Appendix VI

Abbreviations

CSP	Credential Service Provider
DIAS	Digital Identity Acceptance Statement
DIRA	Digital Identity Risk Assessment
FATCA-QI	Foreign Account Tax Compliance Act-Qualified Intermediary
FedRAMP	Federal Risk and Authorization Management Program
GSA	General Services Administration
IAL	Identity Assurance Level
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
TIGTA	Treasury Inspector General for Tax Administration

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

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

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