TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification

September 27, 2023

Memorandum Number: 2023-2S-070

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

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 27, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Memorandum – Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification (Review # 202320013)

This memorandum presents the results of our review of the Internal Revenue Service's (IRS) efforts for the planned implementation of Login.gov's identity verification service. We performed this review during the period December 2022 through September 2023. We plan to continue to evaluate the effectiveness and security of the Login.gov implementation.

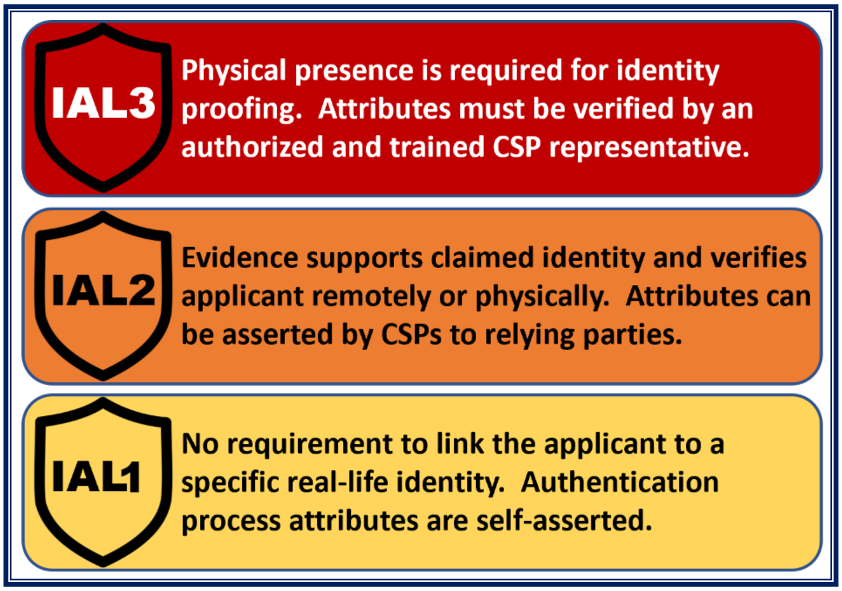
Management's complete response to the draft memorandum is included as Appendix I. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Background

In June 2021, the IRS implemented the Secure Access Digital Identity (SADI) system (replacing Secure Access eAuthentication) as its next-generation identity proofing and authentication solution.[1] According to documentation provided by the IRS, the SADI system employs the National Institute of Standards and Technology (NIST), Special Publication 800-63 Revision 3, *Digital Identity Guidelines* (June 2017), standards. These standards cover identity proofing and authentication of users (*e.g.*, employees, contractors, and private individuals) who interact with Federal Government information systems over open networks, such as the Internet. The IRS built the SADI system with the concept of transitioning to credential service providers (CSP), who are independent and trusted third parties, that issue user authenticators and provide electronic credentials for accessing a system and/or an application (hereafter referred to collectively as applications).

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. Figure 1 summarizes the three IALs established by the NIST and that are used to verify users before granting system access to sensitive information.

Figure 1: Summary of NIST IALs



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

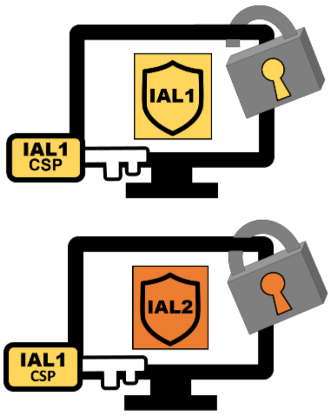
IAL2 **Evidence supports claimed identity and verifies applicant remotely or physically. Attributes can be asserted by CSPs to relying parties.**

IAL1 **No requirement to link the applicant to a specific real-life identity. Authentication process attributes are self-asserted.**

Source: Treasury Inspector General for Tax Administration's (TIGTA) summary of NIST, Special Publication 800-63 Revision 3.

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

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 June 2023, the IRS was leveraging two CSPs for the SADI system, including Login.gov.[2] Login.gov is not IAL2 certified but provides identity proofing services for two IRS IAL1 applications: 1) Form 990-N, Electronic Filing System (e-Postcard) and 2) Foreign Account Tax Compliance Act-Qualified Intermediary.[3]

The General Services Administration (GSA) developed Login.gov to provide identity verification services for Federal Government applications. In 2017, the GSA launched Login.gov allowing individuals to use the same username and password to access public services offered by other participating Federal Government agencies.[4]

According to Login.gov, it verifies the identity of an individual using its own contracted third-party CSPs. When a user creates a Login.gov account, they consent to sharing their sensitive information, such as a Social Security Number, address, telephone number, and driver's license or State identification, for identity proofing. Accordingly, users must upload images of their driver's license or State identification to Login.gov by phone (*i.e.*, cell and smart phones) or computer.[5] These images are retrieved and decrypted only upon the mutual agreement between Login.gov and the partnering Federal Government agency. Login.gov sends [redacted] to the IRS that includes [redacted] during authentication and identity proofing as well as any activities considered important to the security of a user's account. These [redacted] are shared with and accessed only by the IRS, retained for a limited amount of time, and deleted from Login.gov systems once shared.

According to a memorandum issued by IRS executives, they were directed by the Department of the Treasury to consider the use of Login.gov as a CSP. However, the IRS's planning efforts to use Login.gov to authenticate taxpayers to access IAL2 applications created stakeholder concerns. TIGTA's Office of Investigations is responsible for investigating potentially fraudulent activities and other misconduct within IRS programs. As of October 2022, with the use of Login.gov, the IRS [redacted] conducted by TIGTA's Office of Investigations. Prior to using Login.gov, [redacted] from the IRS to TIGTA's Office of Investigations [redacted]. As a result, TIGTA's Office of Investigations has worked with and communicated its concerns to IRS leadership since July 2020, including providing [redacted]. In addition, TIGTA's Office of Investigations was in communication with the

[2] The second CSP (not Login.gov) uses facial recognition technology. The CSP also provides two non-facial recognition options to verify identity: 1) virtual in-person via secure video conference and 2) physically in-person.

[3] Pub. L. No. 111-147, Subtitle A, 124 Stat 97 (codified in scattered sections of 26 U.S.C.).

[4] 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.

[5] If users do not have State-issued identification or cannot complete the step to upload their identification, Login.gov directs the user to contact the partnering Federal Government agency's help center.

IRS and GSA to work on a solution for the [redacted]. However, no solution was implemented and discussions stopped in March 2023.

Objective

The overall objective of this review was to assess the IRS's efforts for its planned implementation of Login.gov.

Results of Review

This memorandum documents the timeline of key events related to the security risks identified with Login.gov and the IRS's planning efforts to implement Login.gov for its IAL2 applications. The timeline covers the period from June 2019 through July 2023. Security risks identified include:

- Login.gov does not comply with NIST IAL2 standards.
- Login.gov has not fully implemented specific controls to improve its anti-fraud program as required by the Office of Management and Budget (OMB).
- Login.gov's [redacted] to TIGTA's Office of Investigations to investigate potentially fraudulent activities.

Summary of Key Events Related to the IRS's Planning Efforts to Implement Login.gov for Its IAL2 Applications

June 2019

The IRS concludes after conducting research that it identified three third-party CSPs providing IAL2 credential services: 1) Login.gov, 2) a CSP that uses facial recognition technology, and 3) another CSP. The CSP using facial recognition technology is the only CSP of the three researched certified as meeting NIST IAL2 standards by an Identity Assurance Assessor.[6] The Identity Assurance Assessor uses an identity assurance framework to provide certifications regarding security standards for electronic identity proofing and credential management services. The IRS recommends procuring and testing all three CSPs to determine which one is best suited for its needs.

January 2020

IRS executives acknowledge that Login.gov is not in compliance with NIST IAL2 standards. IRS leadership meets to discuss that the GSA has not engaged with an independent third-party identity assurance assessor to certify Login.gov at the NIST IAL2 standard.

[6] The Identity Assurance Assessor has assessed industry and Government services since 2010.

July 2020

TIGTA's Office of Investigations engages with the IRS regarding the SADI system and voices concerns about its transition to third-party CSPs, which includes Login.gov. TIGTA's Office of Investigations sends an e-mail to IRS's SADI system management about the IRS [redacted].[7] SADI system management acknowledges TIGTA's Office of Investigations concerns and discusses potential mitigation strategies for Login.gov.

August 2020

The Identity Assurance Assessor begins its evaluation of Login.gov's conformity with NIST IAL2 standards.

September 2020

TIGTA's Office of Investigations participates with the IRS in the initial testing of [redacted] for Login.gov. The testing is designed to gain an understanding of the process and functionality of Login.gov. TIGTA's Office of Investigations requests the test results and [redacted], but neither the IRS nor the GSA provide them.

December 2020

TIGTA's Office of Investigations develops and provides a written document to the IRS that includes recommended [redacted]. If implemented by Login.gov, the [redacted] and help support TIGTA's investigative mission. For nearly two years, TIGTA's Office of Investigations and SADI system management discuss potential mitigation strategies. This results in TIGTA's Office of Investigations cross walking its requirements to what Login.gov can deliver, subsequently updating the document, and resending it to the IRS in March 2021 and June 2022.

June 2021

On June 21, 2021, the IRS implements the SADI system as its next-generation identity proofing and authentication solution.

On June 21, 2021, the IRS launches the Child Tax Credit Update Portal requiring taxpayers to set up an online account with identity verification performed by the CSP that uses facial recognition technology. The CSP also provides two non-facial recognition options to verify identity: 1) virtual in-person via secure video conference and 2) physically in-person.

February 2022

On February 3, 2022, Congress expresses concerns regarding IRS's use of the third-party CSP that uses facial recognition technology to authenticate taxpayers for its online accounts.

On February 7, 2022, the IRS announces that it will transition away from the third-party CSP that uses facial recognition technology and will promptly develop and bring online an additional authentication process that does not use facial recognition technology.

[7] Login.gov provides the capability for individuals to establish a user account at one Federal Government agency and use that same account to access applications at other participating Federal Government agencies.

On February 21, 2022, the IRS announces that the third-party CSP that uses facial recognition technology will now offer taxpayers the option to verify "their identity during a live, virtual interview with agents; no biometric data [(*e.g.*, providing a selfie to a CSP)] – including facial recognition – will be required." The IRS also announces that this is a short-term solution while it works closely with Government partners to roll out Login.gov as an authentication tool.

April 2022

On April 14, 2022, Congress launches an investigation into the third-party CSP that uses facial recognition technology following reports that Americans seeking unemployment benefits faced significant delays due to processing and wait times as well as concerns over privacy and security of the information.

On April 29, 2022, the Identity Assurance Assessor determines that it is unable to issue an IAL2 certification for Login.gov.

July 2022

On July 21, 2022, the IRS and the GSA meet to discuss that Login.gov is to provide sufficient fraud protection and [redacted], but it does not comply with NIST IAL2 standards. IRS documentation supports that the IRS Chief Information Officer (CIO) is obligated to meet the IAL2 standard for Login.gov.

On July 22, 2022, the IRS Login.gov Authorizing Official notifies the IRS CIO that Login.gov does not meet NIST IAL2 standards.

August 2022

TIGTA's Office of Investigations communicates concerns about Login.gov to the IRS.

- On August 5, 2022, TIGTA's Office of Investigations sends e-mails to the IRS SADI system team voicing concerns that Login.gov's [redacted] and Login.gov [redacted].
- On August 9, 2022, TIGTA's Office of Investigations sends an e-mail to IRS Login.gov Authorizing Official expressing concerns about Login.gov's [redacted]. Login.gov will not [redacted] by users during the identity verification process nor will Login.gov [redacted] to the IRS, which have been [redacted] with other SADI system CSPs.

On August 11, 2022, the IRS CIO notes that the GSA will request OMB perform an assessment of Login.gov's security and identity verification controls against NIST IAL2 standards. If these controls are found to be comparable, the OMB will provide written concurrence to the GSA that Login.gov provides a comparable level of security.

On August 18, 2022, the IRS leverages an interagency agreement between the Department of the Treasury and the GSA to use Login.gov. In the interagency agreement, it states that, "Login.gov identity proofing services do not meet NIST IAL2 standards at this time."

On August 22, 2022, the GSA Administrator requests that the OMB's Office of the Federal CIO independently perform a NIST IAL2 conformity review of Login.gov.

> *I am writing today to request an independent review of security and identity verification controls of GSA's Login.gov from the Office of Management and Budget (OMB)'s Office of the Federal Chief Information Officer. The Login.gov team will coordinate with your office to share written evidence to support your independent review, and will be available to answer any questions.*
>
> *Once complete and if in agreement, I request OMB provide written concurrence that Login.gov's proposed fraud and security controls, which do not include a remote biometric comparison, provide a comparable level of security to NIST SP [Special Publication] 800-63-3 Identity Assurance Level 2 (IAL2).*
>
> *My understanding based on an August 11[, 2022] call with the Deputy Director for Management [sic] and the Deputy Secretary of the Treasury [sic] is the Treasury Department will find this concurrence sufficient for GSA's Login.gov to meet its need for identity verification for taxpayer access to Internal Revenue Service (IRS) systems. Additionally, Login.gov's evidence collection process with regard to FAIR evidence employs a method that is implemented and accepted in private industry, but it is not explicitly authorized in a plain text reading of NIST [Special Publication] 800-63-3.*[8]

September 2022

OMB's Office of the Federal CIO assembles a panel of digital identity subject matter experts from within its office and other Federal agencies to review GSA's assertion and supporting documentation that its Login.gov program achieves the intended strength of IAL2 standards as defined by NIST. The Office of the Federal CIO issues the OMB panel's findings to the GSA Administrator. The findings include that Login.gov does not comply with the normative NIST IAL2 guidelines in two key respects.

1. Login.gov does not implement biometric comparison when validating presented identity evidence; therefore, it does not fully comply with the verification of identity evidence as described in NIST, Special Publication 800-63A Revision 3, section 5.3.1.
2. Login.gov does not collect two required "fair" pieces of identity evidence directly from the applicant; therefore, it does not comply with the collection of identity evidence as described in NIST, Special Publication 800-63A Revision 3, sections 4.4.1.2 and 5.2.

The OMB panel also determines that although Login.gov departs, in some ways, from the normative NIST, Special Publication 800-63 Revision 3, the GSA's response demonstrates that its security and identification verification controls achieve the effective strength intended by the NIST IAL2 standards. The OMB further states:

> *However, in order to maintain ongoing confidence in this strength of assurance in the face of evolving threats, Login.gov must continue to ensure that any government programs to which it provides IAL2 services exercise reasonable diligence in actively monitoring registration and attempt data for the purposes of detecting fraudulent identity verification, and that Login.gov can respond to any suspected fraudulent activity identified through this process.*

[8] "Fair" evidence contains at least one reference number that uniquely identifies the person or contains a photograph or biometric template of the person to whom it relates.

The OMB panel's assessment is contingent on Login.gov expanding and improving its anti-fraud program by implementing the following four controls.

1. Login.gov's anti-fraud controls should rely on analysis of identity evidence. [redacted], should be actively monitored for high-risk activity by a dedicated anti-fraud program.
2. Login.gov should establish a retention period and 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.
3. Login.gov should 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.[9]
4. Login.gov should continue to mature its fraud program capabilities, including governance, fraud monitoring, and detection capabilities, as a core program priority.

As of June 7, 2023, Login.gov has not fully implemented any of the OMB panel's anti-fraud controls.

October 2022

On October 11, 2022, TIGTA's Office of Investigations sends a letter to the Deputy Commissioner for Operations Support voicing its concerns with the planned implementation of Login.gov and the potential to [redacted].

> *The purpose of this letter is to provide IRS senior leadership with an understanding of how the transition to third-party CSPs has the potential to* [redacted] *into attacks against, or manipulations of, public facing IRS Internet services. In addition to the potential detrimental impact to Federal tax administration if these Internet services are compromised, there is the significant potential for adverse impact to large volumes of taxpayer records and information, similar to those demonstrated in several exploitations of other IRS services in recent years. Of specific concern is the upcoming, proposed implementation of the Login.gov CSP service under [the] SADI [system], based on our analyses of* [redacted] *with this CSP service.*
>
> [redacted] *the authentication for accounts established and utilized to access taxpayer information on IRS systems,* [redacted]*. Since taxpayer account creation and subsequent accesses were* [redacted]*.*
>
> *By utilizing a CSP,* [redacted]*. As a result, TIGTA potentially* [redacted]*.*

[9] Examples of potential mechanisms can include mailing a notice of the successful proofing event to the registrant's validated postal address or monitoring "dark web" activity regarding fraudulent Login.gov credentials.

On October 19, 2022, the Deputy Commissioner for Operations Support meets with TIGTA's Office of Investigations management, along with GSA and IRS leadership, to discuss concerns raised with the planned implementation of Login.gov. In the meeting, the Deputy Commissioner for Operations Support states that the concerns are not new and are shared by the IRS. In addition, the Deputy Commissioner for Operations Support states that there is no agreement to use Login.gov for Filing Season 2023.

November 2022

On November 7, 2022, IRS executives send a memorandum to the Deputy Commissioner for Operations Support stating that the Department of the Treasury directed the IRS to consider the use of Login.gov as a CSP for Filing Season 2023. The memorandum outlines concerns with Login.gov not being in compliance with NIST IAL2 standards, noting that the use of Login.gov could potentially result in IRS taxpayer data being exploited.

> *The Department of the Treasury (Treasury) directed the IRS to consider the use of Login.gov as a Credent[ial] Service Provider (CSP) for Filing Season 2023. However, GSA, as the CSP for Login.gov, does not provide the IRS with the* [redacted] *to conduct fraud analytics, protect taxpayer information, and combat refund fraud. Additionally, the lack of this data presents challenges for investigative entities, including the TIGTA and IRS Criminal Investigation. The IRS has been proactive in its ongoing communications with GSA regarding the non-conformance of Login.gov service's non-conformance of IAL2 requirements, insufficient front-end fraud detection, and lack of* [redacted]*. These concerns have been shared with Treasury leadership.*
>
> *Login.gov's lack of strong anti-fraud controls prohibits the IRS's ability to detect large-scale exploits, putting billions of dollars of taxpayer payments at risk. The success of the IRS online fraud-fighting effort relies on end-to-end visibility of user's online activity data predicated on a fully complaint IAL2 registration pipeline. Fraud control is mitigation from weaknesses in fully compliant IAL2 implementations. Fraud controls are not a substitute for non-compliant IAL2 implementations. The IRS maintains highly sensitive financial, Personally Identifiable Information (PII) data, and Federal Tax Information (FTI) across the taxpayer community and is a prime target of cyber-fraud. Bad actors have aggressively targeted IRS online applications leveraging identity theft that occurred outside the IRS with compromised third-party information.*
>
> *Adoption of Login[.gov]'s proposed IAL2 solution poses a significant threat to tax administration due to its non-conformance with IAL2 security requirements outlined in the NIST SP [Special Publication] 800-63-3, Digital Identity Guidelines, Revision 3, insufficient front-end fraud detection, and* [redacted] *for investigating fraud schemes. The collective position of the IRS Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer, Former Chief Privacy Officer, and Commissioner of Wage & Investment and Chief Taxpayer Experience Officer is that the use of the IAL2 feature of Login.gov would result in IRS sensitive taxpayer data being exploited.*

On November 8, 2022, the Deputy Commissioner for Operations Support forwards the November 7, 2022, memorandum to the Commissioner of Internal Revenue stating concurrence with IRS executives' concerns for Login.gov. The Deputy Commissioner for Operations Support also states that Login.gov will be available for Filing Season 2023 for IAL1, but not IAL2 applications. In addition, the Deputy Commissioner for Operations Support states that the next window to deploy Login.gov for IAL2 applications is March 2023, if Login.gov is able to satisfy both TIGTA's Office of Investigations and OMB's fraud requirements.

On November 17, 2022, the IRS issues an Authorization to Operate for Login.gov (as a complete system) and moves forward with its plan to implement Login.gov for both IRS IAL1 and IAL2 applications. For example, in January and February 2023, the IRS completes four Login.gov tabletop exercises with GSA personnel to help ensure that responsible individuals know what to do when a critical event occurs, such as suspected fraudulent activity.

On November 17, 2022, Congress releases the results of its investigation of the CSP that uses facial recognition technology to authenticate taxpayers for the IRS and found that the CSP inaccurately overstated its capacity to conduct identity verification services in States that were using it in an attempt to increase service demand.

On November 28, 2022, the IRS CIO notifies the Department of the Treasury's Deputy CIO that the IRS requires the GSA provide an operationally mature fraud capability before the IRS puts IAL2 functionality behind Login.gov. The IRS CIO states that "the IRS will need to see the workflows of these enhanced fraud capabilities and ensure [that] this will meet NIST IAL2 requirements while also addressing IRS and TIGTA concerns."

December 2022

On December 4, 2022, the IRS launches Login.gov to provide identity proofing services for two IRS IAL1 applications and continues its planning to provide identity proofing services for IAL2 applications.

On December 7, 2022, the IRS CIO communicates to the Department of the Treasury's CIO and Deputy CIO that:

> *…[the] IRS is tracking to a mid March 2023 go live for Login.gov IAL2 dependent on receiving final/solid requirements from GSA by 1/13[/2023] and that GSA has completed their fraud enhancements by 2/17[/2023]. If these dependencies are not met, it will impact our schedule. I'll keep you updated – let me know if you need any additional info[rmation]. As you know, this is one of my priorities so I am personally engaged to ensure [that the] IRS is ready.*

On December 17, 2022, the IRS CIO provides a status update on the planned implementation of Login.gov at IAL2 to both the Department of the Treasury's CIO and Deputy CIO. The IRS CIO reports that it is on target for a March 20, 2023, implementation of Login.gov for its IAL2 applications, but it is contingent on Login.gov meeting IAL2-related milestones by early Calendar Year 2023.

January 2023

On January 23, 2023, the IRS CIO communicates to TIGTA's Office of Investigations that "…[the] IRS has been directed by [the Department of the] Treasury to use Login's IAL2 comparable service. Over the last few months, our teams have been working together on the solution to provide TIGTA with the fraud data required. Our teams, along with GSA and [the Department of the] Treasury, will be conducting a tabletop exercise on Tuesday, January 24[, 2023]."

On January 24, 2023, the IRS notifies the GSA that it identified numerous fraud gaps from the tabletop exercise.

On January 24, 2023, in response to the Department of the Treasury's request for a press release to announce the availability of Login.gov, the Deputy Commissioner for Operations Support communicates to the IRS CIO and other IRS stakeholders that, "This message [Regarding: Friday announcement on Login.gov] has to be ve[r]y vague as we have not determined that Login.gov will meet all the fraud/processing requirements. We are optimistic and we are working towards a[n] end of March [2023] deployment, but a lot still has to happen. Standing by to review the release."

On January 25, 2023, the IRS responds to the following question from the U.S. Senate:

> *Question: In your written testimony, you describe how the IRS is working with the GSA to facilitate the use of Login.gov to provide identity authentication of taxpayers who want to access IRS services. What is the timeframe for completing this transition, and does the IRS expect to continue to use any third-party credential service providers once the transition is complete?*
>
> *IRS Response: We continue to engage with [the] GSA to determine when Login.gov will meet IRS requirements. Once the requirements are met, an implementation timeframe may be established. We foresee the need to continue to use third-party CSPs to reduce risk by eliminating reliance on a single CSP and to provide continuity and choice for taxpayers who have already completed the credentialing process.*

Subsequently, in July 2023, the IRS approved the *IRS Credential Service Provider Future State Roadmap* that outlines the need for multiple CSPs.

On January 25, 2023, the IRS Director, Identity Assurance, expresses concerns on the processes and documentation with the GSA's Login.gov fraud program.

On January 29, 2023, the IRS CIO notifies the Deputy Commissioner for Operations Support that:

> *I had previously communicated that [the] IRS was conducting a tabletop exercise with GSA/Login.gov on the fraud processes of Login.gov. The tabletop [exercise] identified numerous gaps in the GSA/Login[.gov] processes that at this point prevent us from moving forward. I am sharing this for awareness as we continue to partner with GSA/Login.[gov]. I will be sharing this update with [the Department of the] Treasury CIO.*

February 2023

On February 17, 2023, the GSA Login.gov Director notifies the IRS Director, Identity Assurance, and the IRS Login.gov Authorizing Official that:

> *To review, we've been working on finding a solution to the following issues:*
>
> *1. Today, Login.gov does not yet add protections for individuals who are at heightened risk of identity theft and for whom standard identity verification controls are insufficient. Specifically, Login[.gov] does not have a technical mechanism to prevent a fraudulent actor from* [redacted].
>
> *2. By design, Login.gov allows* [redacted]. *While there are legitimate circumstances for an individual to have* [redacted] *the practice also allows* [redacted]. *Login[.gov] does not provide a mechanism for subscribers to* [redacted] *on their behalf.*

> *After working with privacy, security, fraud, engineering, and product experts, [the GSA identifies a potential solution to identify and address fraudulent accounts].*[10]

On February 18, 2023, the IRS Chief Privacy Officer sends this information to the Deputy Commissioner for Operations Support and states that, "…the tabletop exercise with the CSP that uses facial recognition technology [sic] and Login.gov on Friday revealed that there are still some critical security gaps with respect to Login.gov."

On February 21, 2023, the IRS CIO notifies both the Department of the Treasury's CIO and Deputy CIO that Login.gov does not include adequate controls to protect against fraudulent activities.

> *The bottom line is that [the] GSA's solution for Login.gov does not include adequate safeguards against fraudulent activity.*
>
> - *Login.gov does not have protections for individuals who are at heightened risk of identity theft because the current solution lacks sufficient verification controls; specifically, Login[.gov] does not have a technical mechanism to prevent a fraudulent actor from* [redacted].
> - *By design, Login.gov allows* [redacted]*; a practice that also allows* [redacted]
> - *Login[.gov] does not provide a mechanism for subscribers to* [redacted] *on their behalf.*
> - *These practices are unacceptable to the IRS and TIGTA because they provide an avenue for increased undetected fraudulent activity against current and future IRS taxpayers.*

March 2023

On March 7, 2023, the GSA Office of Inspector General issues an audit report outlining how the GSA misled Login.gov customers that it is NIST IAL2 certified.[11]

On March 8, 2023, the Department of the Treasury announces that its Deputy CIO will move to the IRS to become the Acting CIO, and the IRS's CIO will move to the Department of the Treasury to become the Chief Technology Officer, both effective March 27, 2023.[12]

On March 8, 2023, the IRS CIO and other IRS executives prepare a Login.gov Go/No-Go decision document that provides their assessment of Login.gov's overall readiness for a March 20, 2023, implementation. In the Go/No-Go decision document, the IRS provides the "readiness assessment" of four areas: Business, Cybersecurity, Privacy and Information Protection, and Technical. The Go/No-Go decision document states that Login.gov is "Not Ready" for

[10] Bracketed language is TIGTA's summary to protect sensitive information.

[11] GSA, Office of Inspector General, JE23-003, *GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards* (Mar. 2023).

[12] Nextgov/Federal Computer Week, *[sic] Currently Deputy Chief Information Officer at Treasury, Will Be Taking On the Role of Acting CIO at the IRS* (Mar. 2023). On June 14, 2023, the IRS announces that the IRS's Chief Technology Officer will become the new IRS Acting CIO. The previous IRS Acting CIO will return to the Department of the Treasury as its Deputy CIO. Both transfers are effective July 3, 2023.

implementation in three of the four readiness assessment areas. Examples provided to support the readiness assessment include the following:

- Business Readiness Assessment – “GSA Login.gov allows for [redacted], which increases [the] likelihood of identity theft and fraud. The taxpayer may think that [redacted] to them, while a fraudster can [redacted].”
- Cybersecurity Readiness Assessment – “The CSP serves as the first line of defense to stop fraud of IRS taxpayers. GSA Login.gov currently lacks a formal fraud detection and remediation operation.”
- Privacy and Information Protection Readiness Assessment – “The lack of Login.gov’s fraud controls, including [redacted], and the inability for Login.gov to [redacted], creates undue risk to IRS systems and potential unauthorized disclosure of confidential taxpayer data. We should not deploy processes that lack the strong security requirements required to protect taxpayer data and IRS systems.”

The IRS CIO and other IRS executives did not make a Go/No-Go decision nor did they sign the Go/No-Go decision document. In an e-mail, the IRS CIO notifies the Deputy Commissioner for Operations Support that:

> *[T]he IT [Information Technology] team is collaborating across the IRS to present a Login.gov Go/No-Go for the Deputy Commissioners. Given the recent IG [Inspector General] report and the interest from [the Department of the] Treasury, I believe it is in the best interest of the IRS to defer the Go/No-Go [decision] until the [Department of the] Treasury selected Acting CIO onboards. As a result, I am asking the IT team to continue to create the briefing document for a discussion after March 17[, 2023].*

When asked to clarify whether the Go/No-Go decision meeting scheduled for March 13, 2023, should be re-scheduled for a date after March 17, 2023, the IRS CIO instructs the IRS Login.gov Authorizing Official to “stand down until the acting CIO provides his perspective.” Subsequently, the Go/No-Go decision meeting was canceled and was never re-scheduled.

On March 8, 2023, the IRS Login.gov Authorizing Official notifies the IRS CIO that:

> [redacted]

> [redacted]

On March 9, 2023, the IRS CIO responds to the IRS Login.gov Authorizing Official that:

> [redacted]

> [redacted]

> [redacted]

Subsequently, on that same day, the IRS Chief Privacy Officer also responds that "I have significant concerns about subjecting 10,000 taxpayers to the risks we've identified before the Go/No-Go [decision]."

On March 13, 2023, the Department of the Treasury's Deputy CIO sends via e-mail to the Deputy Commissioner for Operations Support [redacted]?"

On March 16, 2023, the Department of the Treasury and the GSA modify the Login.gov contract to add "anticipated usage of identity verification services" for approximately $18 million, bringing the total contract amount to nearly $22.6 million.

On March 17, 2023, the IRS Login.gov Authorizing Official communicates to the IRS Deputy CIO of Operations, who concurs, that "my understanding is the planned integration with Login.gov has been postponed and will not occur on March 20, 2023, as planned."

On March 23, 2023, the GSA notifies the IRS that GSA would postpone the planned implementation of Login.gov for IRS IAL2 applications. The GSA cites risks associated with deploying Login.gov during peak processing of the IRS's filing season and the lack of an agreement between the IRS and Login.gov to share taxpayer data. On the same day, the IRS Acting CIO notifies IRS stakeholders of the GSA's decision to postpone, and states, "We may revisit the implementation schedule once filing season is complete."

On March 24, 2023, the IRS Director of Communications responds to the Department of the Treasury's Deputy CIO regarding the IRS and the GSA's statements that the IRS is delaying Login.gov implementation of its IAL2 applications, stating that:

> *…their statement does not make it clear that this was a GSA decision. But I think, when paired with the IRS statement noting it was GSA, that helps address that piece of it. The view over here remains that we shouldn't be implying or suggesting it's our volume of work driving this decision, so we need to skip the 'peak processing' reference.*

On March 27, 2023, the IRS Acting CIO communicates to the Deputy Commissioner for Operations Support and Chief Privacy Officer that "…we should expect there to be a continued push for Login.gov over at OMB. There was a meeting this weekend between [the Department of the] Treasury/GSA/OMB and they intend to push for deployment before 04/18[/2023]."

On March 27, 2023, the IRS Chief Privacy Officer communicates to the IRS Acting CIO and the Deputy Commissioner for Operations Support that:

> [redacted]

Subsequently, on the same day, the IRS Acting CIO responds to the IRS Chief Privacy Officer that "I'm only flagging the outside pressure for general awareness, as it would not surprise me if this landed in the Commissioner[']s lap."

On March 27, 2023, the IRS Chief Privacy Officer communicates to the Deputy Commissioner for Operations Support that a news release from the Department of the Treasury regarding the postponement of the planned deployment of Login.gov at the IRS "…does not reflect our conversation on Friday [March 24, 2023]."[13]

On March 28, 2023, the IRS Acting CIO communicates to the Deputy Commissioner for Operations Support that:

> *Agreement over the weekend is consistent with what I mentioned below – [meaning the] move forward at some point during filing season [2023]. [The Department of the] Treasury/GSA MOU [Memorandum of Understanding] will contain references to the OMB IAL2 opinion. The 6103 agreement still rests with [the] GSA but should be coming across for IRS review. TIGTA comments for their MOU are being adjudicated by [the Department of the] Treasury. We should probably catch the CIR [Commissioner of Internal Revenue] up at some point.*

On March 28, 2023, the IRS Acting CIO notifies the Login.gov Authorizing Official that "…there will continue to be a push for Login.gov [for IRS IAL2 applications at] 10,000 users before 04/18[/2023]."

On March 29, 2023, the Congressional Committee on Oversight and Accountability, Subcommittee on Government Operations and the Federal Workforce, holds a hearing, "Login.gov Doesn't Meet the Standard." Testimonies are given concerning the findings from the GSA Office of Inspector General report on Login.gov. Witnesses include representatives from the GSA Office of Inspector General, Login.gov, and the NIST.

On March 31, 2023, IRS documentation supports that IRS planning efforts continue for the implementation of Login.gov for its IAL2 applications with a limited scope launch for up to

[13] Government Executive, *Planned Login-dot-gov Deployment at IRS is Postponed* (Mar. 2023).

10,000 users. Plans include performing analysis on the results of the 10,000 users, and that "a decision will be made based on the outcomes of the analysis."

April 2023

On April 3, 2023, the Department of the Treasury's Associate CIO, Enterprise Infrastructure Operations Services, notifies the IRS Director, Identity Assurance, that "we are not doing the limited scope launch this tax season," because the GSA has not delivered on the Interagency Agreement and there is "quite a bit of controversy to be addressed."

As of April 12, 2023, according to e-mail communications provided by the IRS, the IRS and Login.gov continue to develop a Memorandum of Understanding to include appropriate provisions to protect shared taxpayer data.[14]

As of April 28, 2023, according to e-mail communications provided by the IRS, it has not worked on Login.gov since the GSA postponed the planned implementation of Login.gov for IRS IAL2 applications on March 23, 2023.

May 2023

On May 10, 2023, the Department of the Treasury and the GSA modify the Login.gov contract to "support an additional application" related to IAL1 identity proofing for approximately $43 thousand, bringing the total contract amount to nearly $22.6 million.

On May 12, 2023, the Department of the Treasury and the GSA modify the Login.gov contract to "return funds due to revised cost estimates for projected [Login.gov] usage" for approximately $22.4 million, bringing down the total contract amount to approximately $240 thousand.

On May 12, 2023, IRS leadership and TIGTA's Office of Investigations management meet to discuss the "test plan" for the [redacted] if the postponed implementation of Login.gov is lifted. The test plan with gap analysis will be sent out for feedback.

July 2023

The IRS approves the *IRS Credential Service Provider Future State Roadmap* that outlines the need for two or more CSPs, including a Government and non-Government option, to provide taxpayers with a choice of CSP service based on the taxpayer's preference.

Conclusion

This summary of documented key events supports 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. These concerns included not effectively implementing security controls that incorporate compliance with NIST IAL2 standards, fully implementing OMB's anti-fraud program, and making [redacted]. According to IRS senior leadership, the

[14] The Memorandum of Understanding would include information based on 26 U.S. Code § 6103 – *Confidentiality and Disclosure of Returns and Return Information*.

IRS would not implement Login.gov until these requirements were met. Furthermore, the IRS Acting CIO communicated to IRS executives that the OMB, the GSA, and the Department of the Treasury were continuing to push for the deployment of Login.gov. The IRS continued to expend limited resources towards planning efforts for its IAL2 applications after the GSA postponed Login.gov's implementation. As previously mentioned, we plan to continue to evaluate the effectiveness and security of the Login.gov implementation.

Performance of This Review

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Federal Offices of Inspector General*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented.

Major contributors to the review were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Catherine Sykes, Audit Manager; David Allen, Lead Auditor; Carreen Diaz, Auditor, and Amin Sejtanic, Auditor.

Appendix I

Management's Response to the Draft Memorandum

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

DEPUTY COMMISSIONER

September 22, 2023

MEMORANDUM FOR HEATHER M. HILL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Jeffrey J. Tribiano Jeffrey J. Tribiano Digitally signed by Jeffrey J. Tribiano Date: 2023.09.22 08:22:01 -04'00'
Deputy Commissioner for Operations Support

SUBJECT: Draft Memorandum – Review of the Internal Revenue Service's Planned Implementation of Login.gov (Review # 202320013)

Thank you for the opportunity to respond to the above-referenced draft memorandum. We appreciate the TIGTA audit team's engagement with IRS leadership to ensure that the memorandum accurately reflects the facts related to the planned implementation of Login.gov and actions taken by the IRS.

The protection of taxpayer information is a top priority for the IRS, and we strive daily to improve our processes and maintain the public's confidence. We also strive to enhance the taxpayer experience within the constraints of protection of taxpayer information. We continue to work towards a technical solution that will satisfy both.

If you have any questions, please contact me or a member of your staff may contact Kathleen Walters, chief privacy officer, at 202-317-4082.

Appendix II

Glossary of Terms

Term	Definition
[redacted]	[redacted]
[redacted]	[redacted]
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.
Calendar Year	Twelve (12) consecutive months ending December 31.
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.
Chief Technology Officer	An executive information technology position that involves developing and implementing new technologies, and provides technical review and oversight.
Child Tax Credit Update Portal	Allows taxpayers to elect out of receiving payments related to the Advance Child Tax Credit and to provide updates to the number of qualifying children, marital status, or significant change in the taxpayer's income. It was officially decommissioned and retired on May 9, 2022.
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.
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.

Term	Definition
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	A secure web-based platform that enables users to apply, renew, or terminate an existing agreement and manage their information.
Go/No-Go Decision	The decision as to whether or not to proceed as planned.
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.
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.
Milestone	A management decision point placed at a natural breakpoint in the life cycle, at the end of the phase, where management determines whether a project can proceed to the next phase.
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.
Secure Access Digital Identity	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.
Secure Access eAuthentication	An IRS system that collects Personally Identifiable Information to validate and authenticate taxpayers who attempt to access IRS services via the Internet.
Tabletop Exercise	The incidence response 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.
Treasury Inspector General for Tax Administration's Office of Investigations	Its overall mission is to help protect the ability of the IRS to collect revenue for the Federal Government. It conducts investigations and proactive investigative initiatives to ensure the integrity of IRS employees, contractors, and other tax professionals; ensure IRS employee and infrastructure security; and protect the IRS against external attempts to corrupt tax administration.

Appendix III

Abbreviations

CIO	Chief Information Officer
CSP	Credential Service Provider
GSA	General Services Administration
IAL	Identity Assurance Level
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SADI	Secure Access Digital Identity
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.