



Report to the Chairman of the  
Subcommittee on Oversight, Committee  
on Ways and Means, House of  
Representatives

---

June 2025

# TAXPAYER IDENTITY VERIFICATION

## IRS Should Strengthen Oversight of Its Identity-Proofing Program

# GAO Highlights

Highlights of [GAO-25-107273](#), a report to the Chairman of the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

## Why GAO Did This Study

IRS offers more than 30 online applications to help taxpayers meet their tax obligations. To guard against fraud and abuse, IRS requires users to prove their identities when accessing these applications. This process can require users to divulge sensitive personal information about themselves.

GAO was asked to review IRS's identity-proofing program. This report assesses how IRS monitors and oversees the performance of its identity-proofing program.

GAO reviewed IRS policies and procedures associated with IAL2 identity proofing; interviewed relevant IRS officials and ID.me staff; and reviewed ID.me-related performance data and contract information.

## What GAO Recommends

GAO is making four recommendations to IRS, including (1) defining and documenting measurable goals and objectives for its identity-proofing program; (2) regularly evaluating and documenting the results of its identity-proofing program; and (3) ensuring that procured identity-proofing solutions that involve the use of AI included in IRS's AI inventory are consistent with applicable legal requirements and are subject to IRS's AI oversight process. IRS agreed with all of the recommendations.

For more information, contact James R. McTigue, Jr., at [mctiguej@gao.gov](mailto:mctiguej@gao.gov).

June 2025

## TAXPAYER IDENTITY VERIFICATION

### IRS Should Strengthen Oversight of Its Identity-Proofing Program

## What GAO Found

Federal agencies identify and verify that users attempting to access government services, benefits, and other resources are who they claim to be. This identity-proofing process may occur in person, by telephone, or online. The National Institute of Standards and Technology has issued guidance defining three risk-based identity-assurance levels for online interactions: (1) some confidence of claimed identity, (2) high confidence, and (3) very high confidence.

In implementing its identity-proofing program, the Internal Revenue Service (IRS) determined that it needed identity assurance level (IAL) 2 in providing users access to certain online IRS applications. A private credential service provider, ID.me, is IRS's sole provider of level 2 identity-proofing products and supporting activities. These activities include having individuals provide evidence, such as a driver's license, and biometric evidence, such as a selfie (see figure).

#### High-Level Identity Assurance Level 2 Digital Identity-Proofing Process



Sources: GAO analysis and illustrations (license, Social Security card, hand/phone icons); Golden Sikorka/stock.adobe.com (laptop); viktorijareut/stock.adobe.com (passport). | GAO-25-107273

The reach of IRS's digital identity-proofing program is considerable—users accessed IAL 2 applications more than 150 million times between 2021 and 2024, according to IRS data.

IRS is conducting several oversight activities to monitor ID.me and overall program performance. These include (1) issuing 12 directives to ID.me on ensuring its solutions protect users' privacy; (2) documenting data validation checks to determine if ID.me is adhering to contract terms and conditions; and (3) holding biweekly meetings with vendor representatives to discuss challenges, performance, and associated issues.

However, gaps remain in IRS's oversight of its identity-proofing program:

- IRS was unable to show it had measurable goals and objectives for the program. IRS receives performance data from the vendor but did not show it independently identified outcomes it is seeking. IRS also has not shown documented procedures to routinely evaluate credential service providers' performance. Without stronger performance reviews, IRS is hindered in its ability to take corrective actions as needed.
- ID.me acknowledges that its identity-proofing process involves the use of artificial intelligence (AI) technologies. However, IRS has not documented these uses in its AI inventory or taken steps to comply with its own AI oversight policies. Doing so would provide greater assurance that taxpayers' rights are protected and that the technologies are accurate, reliable, effective, and transparent.

---

# Contents

---

Letter		1
	Background	3
	IRS Has Taken Steps to Protect Users' Privacy and Monitors Aspects of ID.me's Performance, but Gaps Remain in Program Oversight	14
	Conclusions	21
	Recommendations for Executive Action	21
	Agency Comments	22
Appendix I	Objectives, Scope, and Methodology	23
Appendix II	IRS Applications Requiring Identity-Proofing	26
Appendix III	Comments from the Internal Revenue Service	28
Appendix IV	GAO Contact and Staff Acknowledgments	30
Tables		
	Table 1: Identity Assurance Levels (IAL) as Defined by the National Institute of Standards and Technology	4
	Table 2: Internal Revenue Service Applications Requiring Identity Assurance Level (IAL) 1 and 2 Identity Proofing	26
Figures		
	Figure 1: Identity Proofing Balances Privacy, Security, and Usability	6
	Figure 2: Digital Taxpayer Identity-Proofing Process for Internal Revenue (IRS) Service Identity Assurance Level 2 Online Applications	9
	Figure 3: Timeline of Key Taxpayer Identity-Proofing Events at the Internal Revenue Service (IRS)	10

---

---

## Abbreviations

AI	artificial intelligence
BPA	blanket purchase agreement
CSP	credential service provider
EO	executive order
FISMA	Federal Information Security Modernization Act of 2014
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
PII	personally identifiable information
SADI	Secure Access Digital Identity

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



June 11, 2025

The Honorable David Schweikert  
Chairman  
Subcommittee on Oversight  
Committee on Ways and Means  
House of Representatives

Dear Mr. Chairman,

The Internal Revenue Service (IRS) provides taxpayers with access to more than 30 online applications to help them meet their tax obligations. According to IRS data, users accessed these applications—such as individual online accounts—more than 150 million times between June 2021 and November 2024. IRS uses digital identity-proofing processes and IT systems to increase assurance that these applications are secure and transactions are conducted only with authorized individuals.<sup>1</sup> Identity proofing for most IRS applications requires personally identifiable information (PII) to be collected from taxpayers and businesses to verify their identities.

Robust identity proofing is critical because unauthorized and fraudulent access to PII and taxpayer accounts poses constant risks. IRS estimates billions of dollars in fraudulent payments are made each year. For example, in fiscal year 2024, IRS identified over \$9.1 billion in fraud from tax and financial crimes and seized criminal assets totaling approximately

---

<sup>1</sup>In general, identity proofing is the process by which credential service providers verify individuals' identities before allowing them access to sensitive data, such as tax return information from a prior year or the status of a tax refund. Identity proofing ensures that users are who they claim to be. The term "authentication" refers to the process of ensuring that returning users are still who they claim to be. IRS uses identity proofing before allowing individuals or businesses access to a resource, such as an IT system. A credential service provider is a trusted entity that verifies and authenticates users' identities and issues electronic credentials to subscribers, such as IRS.

---

\$1.2 billion.<sup>2</sup> Our prior work has found that strong internal controls can help IRS protect PII and detect and prevent tax fraud.<sup>3</sup>

Since June 2021, IRS's highest-risk identity-proofing needs have been supported by ID.me, a private credential service provider (CSP).<sup>4</sup> IRS uses ID.me to provide identity proofing for dozens of taxpayer applications, such as individual online IRS accounts. This allows taxpayers to access account information including their balances, payments, and tax records.

You asked us to describe how IRS manages its identity-proofing program. This report assesses the extent to which IRS monitors and oversees the performance of the program.

To address our objective, we reviewed documentation on how ID.me conducts digital identity proofing. We also reviewed documentation on federal guidelines and IRS policies related to identity proofing. We interviewed relevant IRS and Department of the Treasury officials as well as officials from ID.me. We also interviewed officials from V3Gate, the reseller of ID.me's identity-proofing products.<sup>5</sup> We reviewed academic literature, government reports, and industry white papers to identify what is known about taxpayer identity proofing. We also conducted semi-structured interviews with selected knowledgeable stakeholders about identity-proofing programs, services, and technology.

Furthermore, we reviewed ID.me data and ID.me-related contract documentation. We collected and analyzed documentation on available

---

<sup>2</sup>Internal Revenue Service, *IRS Criminal Investigation releases FY24 Annual Report; details agency's global reach, billion-dollar impact*, IR-2024-307 (Dec. 5, 2024).

<sup>3</sup>See GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, [GAO-18-418](#) (Washington, D.C.: June 22, 2018); and *Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks*, [GAO-15-119](#) (Washington, D.C.: Jan. 20, 2015).

<sup>4</sup>IRS also uses Login.gov, a federally run CSP, to authenticate lower-risk digital interactions.

<sup>5</sup>V3Gate is a reseller of ID.me identity-proofing software licenses and support services. Resellers are intermediaries between the service/product manufacturers and consumers which operate in software, service, and manufacturing industries. In this case, V3Gate's customers are Treasury and IRS, while the vendor is ID.me. IRS places delivery and task orders against a Treasury blanket purchase agreement (BPA) and government-wide acquisition contract with V3Gate for ID.me-provided identity-proofing software licenses and support services.

---

information, procedures, and activities that IRS uses to monitor identity proofing performed by ID.me solutions.<sup>6</sup> We assessed the reliability of ID.me performance and contract data by reviewing documents, discussing data reliability methods used with those responsible, and examining the data for internal consistency or anomalies. We found the data to be reliable for the purpose of analyzing ID.me performance monitoring and contract obligations. We compiled criteria based on standards for internal controls in the federal government.<sup>7</sup> We then compared these criteria to the documentation and interviews we conducted with IRS officials in charge of monitoring these activities. Finally, we met with Treasury and IRS officials and staff from V3Gate and ID.me who are knowledgeable about relevant identity-proofing contracts and artificial intelligence (AI) oversight requirements. We also reviewed relevant federal and agency requirements for AI and IRS's public and internal inventories of its use of AI. Appendix I provides more detail on the objective, scope, and methodology that guided our work.

We conducted this performance audit from January 2024 to June 2025 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 objectives. We believe that the evidence obtained provides a reasonable basis for any findings and conclusions based on our audit objectives.

---

## Background

### Federal Laws and Guidance

Federal laws and guidance specify requirements and recommendations affecting IRS's identity proofing, including:

- The Privacy Act of 1974 establishes agency responsibilities and protections for personal information accessed or held by federal agencies.<sup>8</sup> For example, the Privacy Act limits the collection, disclosure, dissemination, and use of personal information maintained

---

<sup>6</sup>For purposes of this report, the term "solutions" refers to ID.me licenses and support services procured under the BPA with V3Gate, which IRS describes as including the provision of Identity Assurance Level 2 self-service digital identity-proofing credentials for access to IRS applications, remote live video sessions, antispoofing detection, and in-person kiosk proofing licenses, among others. When we refer to ID.me performance under the BPA, we are referring to the performance of ID.me's identity-proofing solutions.

<sup>7</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

<sup>8</sup>5 U.S.C. § 552a.

in “systems of records,” or groups of records under the control of any agency from which information is retrieved by individual name or identifier.

- The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or managed by another entity.<sup>9</sup>
- In 2017, the National Institute of Standards and Technology (NIST) issued guidance on identity proofing.<sup>10</sup> This guidance defined three Identity Assurance Levels (IAL), which describe the degree of confidence that a user’s claimed identity is their real identity. NIST recommends agencies choose an assurance level based on their respective risk profiles and the potential harm from an attacker falsely claiming an identity. IRS applies the NIST standards to determine whether applications are IAL1, 2, or 3, in part, based on the sensitivity of information they hold, such as Social Security numbers, and the potential harm caused if an attacker gained access to the system (see table 1).

**Table 1: Identity Assurance Levels (IAL) as Defined by the National Institute of Standards and Technology**

IAL level	Description	Evidence collected
IAL1	There is no requirement to link users to a specific real-life identity. Any information provided by users should be treated as self-asserted and is neither validated nor verified.	None.
IAL2	The evidence provided verifies that users are appropriately associated with a real-world identity. This level introduces the need for either remote or physically present identity proofing.	Evidence may include a passport or driver’s license, and remote biometric evidence, such as a selfie.
IAL3	Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained credential service provider representative.	Passport and driver’s license, and physical or remote interaction supervised by a live operator.

Source: GAO analysis of National Institute of Standards and Technology, Special Publication 800-63 Revision 3. | GAO-25-107273

<sup>9</sup>44 U.S.C. § 3354(b). The Federal Information Security Modernization Act of 2014 (FISMA 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002. Pub. L. No. 113-283, 128 Stat. 3073 (2014); Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

<sup>10</sup>National Institute of Standards and Technology, *Digital Identity Guidelines*, Special Publication 800-63-3 and *Digital Identity Guidelines: Enrollment and Identity Proofing*, Special Publication 800-63A (June 2017).



---

NIST also provides standards for identity-proofing security and privacy. The NIST Privacy Framework includes a set of guidelines designed to help IRS (and other organizations) identify, manage, and mitigate privacy risks associated with collecting and using PII and implementing safeguards to protect it.<sup>11</sup>

Additionally, certain requirements affect how IRS is to oversee contractors' use of AI, such as biometric data matching that can be used for identity proofing. Executive Order (EO) 13960 and the Advancing American AI Act require most agencies to document uses of AI, including contracted AI, in a central agency inventory.<sup>12</sup> Identity-proofing processes can use AI technologies, including biometric data matching technologies (e.g., facial recognition). However, IRS internal guidance requires each AI application to align with certain principles in EO 13960, such as being accurate, reliable, effective, and transparent.<sup>13</sup>

---

## Balancing Privacy, Security, and Usability

Agencies, such as IRS, that conduct identity proofing must balance tradeoffs among three needs: privacy, security, and usability. If IRS makes the identity-proofing process too stringent, legitimate taxpayers may not be able to successfully prove their identities and access services or account information. Conversely, if the process is too easy for users to

---

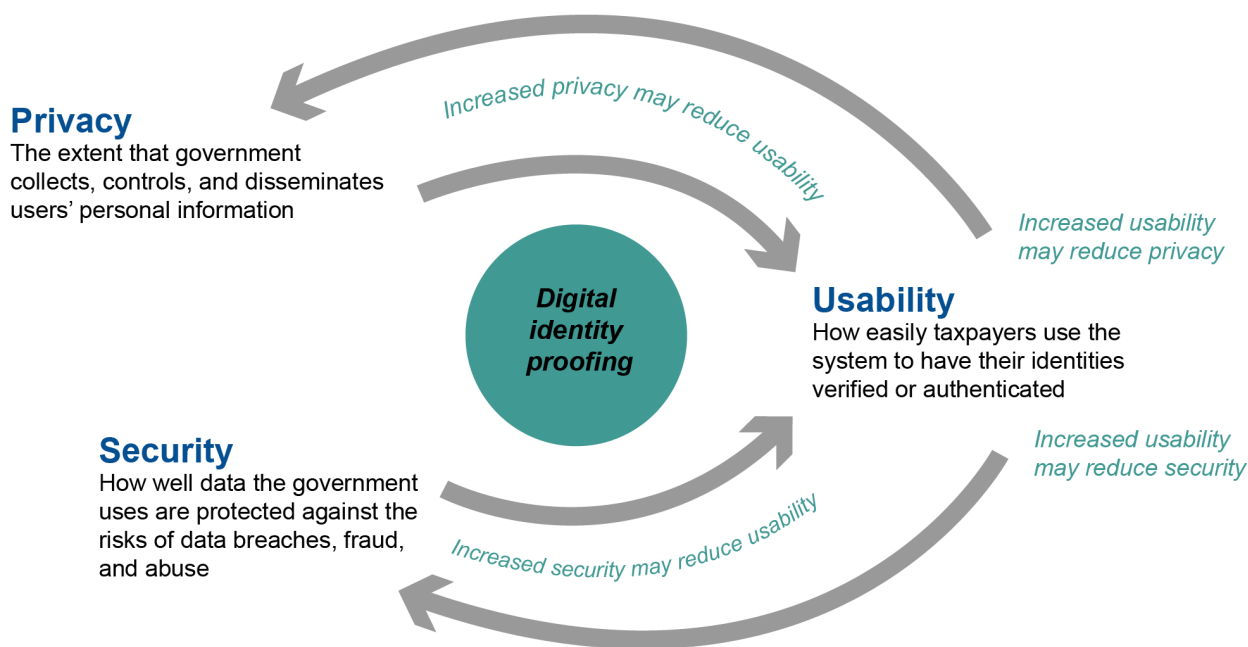
<sup>11</sup>National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0 (Jan. 16, 2020). For more details on IAL standards and their application, see GAO, *Identity Verification: GSA Should Fully and Promptly Establish Data Protection Policies and Procedures for Login.gov*, [GAO-25-107000](#) (Washington, D.C.: June 3, 2025).

<sup>12</sup>Exec. Order No. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 85 Fed. Reg. 78939 (Dec. 8, 2020); James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, §§7221-7228, 136 Stat. 3668-3676 (2022) (*reprinted* in 40 U.S.C. § 11301 note). The executive order and law include some exclusions.

<sup>13</sup>In May 2024, IRS issued an interim AI governance policy that established an oversight process for AI, including contracted AI. That guidance was based in part on Executive Order 14110, which was rescinded in January 2025. In March 2025, IRS issued an updated interim policy for AI Governance which superseded the May 2024 guidance. For more detail, see IRS Interim Guidance Memorandum (RAAS-10-0325-0001), Interim Policy for AI Governance (Mar. 11, 2025); Exec. Order No. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 85 Fed. Reg. 78939 (Dec. 8, 2020); Exec. Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed. Reg. 75191 (Nov. 1, 2023); and Exec. Order No. 14179 *Removing Barriers to American Leadership in Artificial Intelligence*, 90 Fed. Reg. 8741 (Jan. 31, 2025). In addition, Executive Order 14179 requires the development of an AI Action Plan by July 22, 2025.

pass, then IRS's identity proofing may be more susceptible to a host of security failures including unauthorized access and fraud (see fig. 1).

**Figure 1: Identity Proofing Balances Privacy, Security, and Usability**



Source: GAO analysis of National Institute of Standards and Technology guidelines, Internal Revenue Service's Privacy Program Plan, and Office of Management and Budget guidance. | GAO-25-107273

**Privacy.** NIST defines privacy as the freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. According to IRS's Privacy Program Plan, privacy controls are the safeguards employed to manage privacy risks, ensure compliance with applicable privacy requirements, and maintain the integrity and confidentiality of personally identifiable information (PII).<sup>14</sup>

**Security.** Security is defined as protection against the risks of data breaches, fraud, and abuse. According to IRS's Privacy Program Plan, security controls are the safeguards or countermeasures employed to

<sup>14</sup>Internal Revenue Service, *Privacy Program Plan*, Publication 5499, Rev. 2-2024, (Dec. 31, 2023).

---

protect the confidentiality, integrity, and availability of a system and its information and to manage information security risk.

**Usability.** Usability is defined as ensuring that use of a government service is not stressful, confusing, or daunting.<sup>15</sup> According to the Office of Management and Budget (OMB), federal websites and digital services that require identity proofing should be both secure and easy to access.<sup>16</sup>

In balancing privacy and security concerns, IRS and CSP officials told us they attempt to limit the taxpayer information they request and, in most cases, are required to destroy the information after using it to prove the identity of taxpayers.

The personal information provided by users in the identity-proofing process is used to detect and block potentially fraudulent users from accessing IRS digital applications. IRS officials and ID.me staff told us that access to IRS applications for these users was suspended pending further review and verification.

However, taxpayer advocacy groups, trade associations, and tax preparers have expressed concerns about how CSPs, including ID.me, acquire and use taxpayers' PII, particularly the potential use of facial recognition technology, biometric data, and other sensitive information. According to these groups, the more personal information and biometric data collected by CSPs, the more risk that personal data could be compromised should a privacy incursion occur at the CSP.<sup>17</sup> In contrast, ID.me officials said that broader use of biometrics reduces fraud and can be done in a responsible manner to reduce privacy incursions and protect individuals. ID.me officials also said that properly deployed biometrics can help CSPs prevent more fraud.

These stakeholders have also raised concerns about identity proofing's growing burden and effect on usability. For example, efforts to enhance privacy protections and maintain security over PII can further complicate

---

<sup>15</sup>This definition is based on the Office of Management and Budget's Digital Services Playbook, accessed July 10, 2024.

<sup>16</sup>Office of Management and Budget, *Delivering a Digital-First Public Experience*, M-23-22 (Sept. 22, 2023).

<sup>17</sup>For more on issues related to biometrics, see GAO, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns*, GAO-24-106293 (Washington, D.C.: Apr. 22, 2024).

---

the digital identity-proofing process by requiring users to complete multiple steps, upload documents, and fill in forms with detailed personal information.

Changing technology is further complicating identity proofing. According to NIST, when organizations attempt to prove users' identities remotely via a web application, they face risks of impersonation or other attacks.<sup>18</sup> Solutions to this problem include liveness detection, a technique to verify if a person presenting a biometric is a live human being, rather than a fake image or recording. However, digital identity proofing can affect individuals' privacy through the transmittal and use of sensitive PII.

---

## The Digital Identity-Proofing Process

Digital identity proofing is the process through which a CSP collects and verifies information about a person for the purpose of issuing credentials to that user. To complete verification for IAL2 applications, at a minimum, an individual will need access to a computer or mobile phone that has a camera, an email address, and a valid government-issued photo ID, among other sources of information.<sup>19</sup> Figure 2 depicts the tasks required to complete this process.<sup>20</sup>

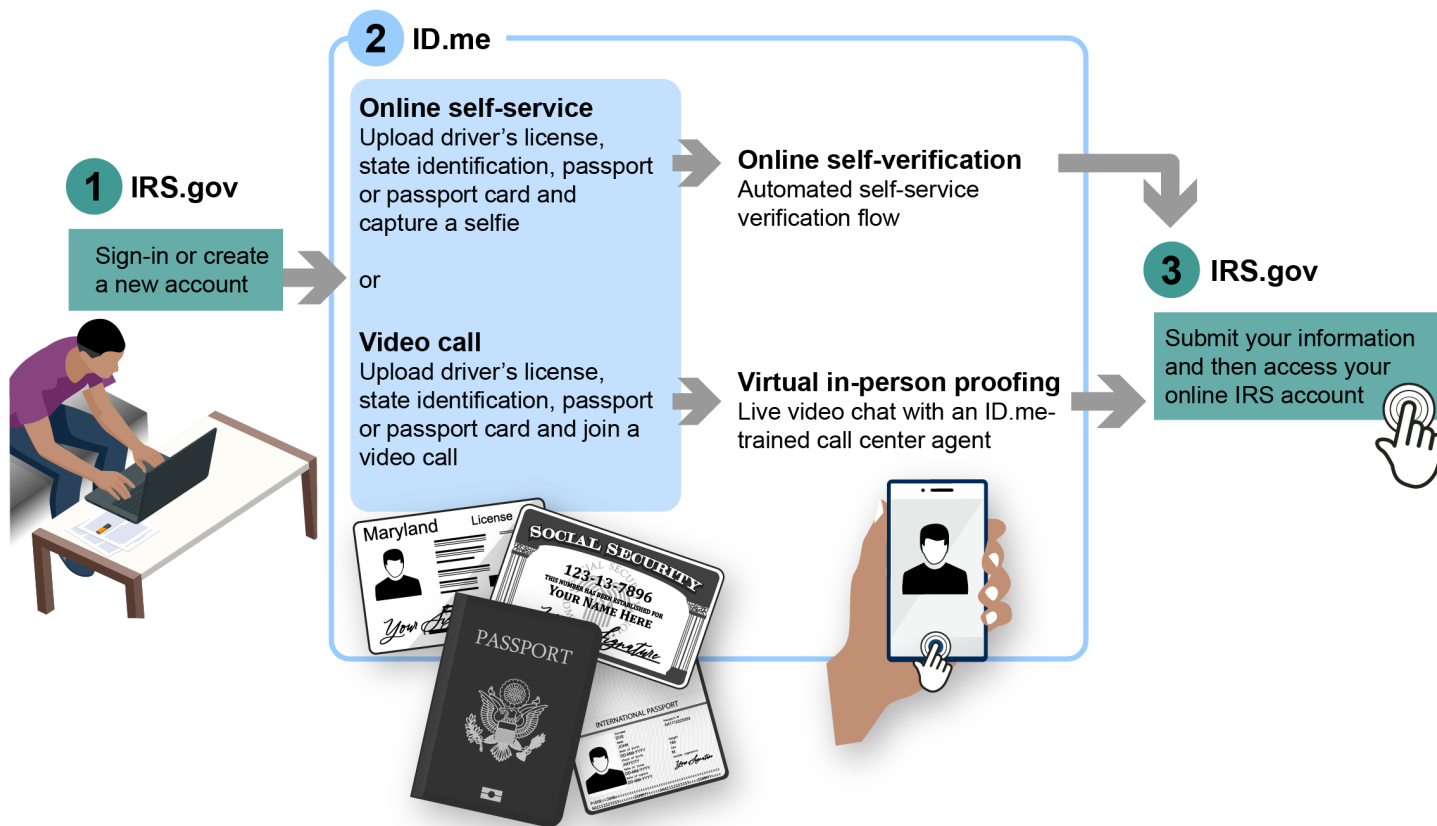
---

<sup>18</sup>National Institute of Standards and Technology, *Digital Identity Guidelines*, Special Publication 800-63-3 and *Digital Identity Guidelines: Enrollment and Identity Proofing*, Special Publication 800-63A (June 2017).

<sup>19</sup>Taxpayers who cannot complete the identity-proofing process online have the option to use nondigital options, such as visiting a taxpayer assistance center or speaking with an IRS representative over the phone.

<sup>20</sup>For a more detailed description of this process, see [GAO-25-107000](#), and *Identity Verification: GSA Needs to Address NIST Guidance, Technical Issues, and Lessons Learned*, [GAO-25-106640](#) (Washington, D.C.: Oct. 16, 2024).

**Figure 2: Digital Taxpayer Identity-Proofing Process for Internal Revenue (IRS) Service Identity Assurance Level 2 Online Applications**



Sources: GAO analysis and illustrations (license, Social Security card, hand/phone icons); Golden Sikorka/stock.adobe.com (person); viktorijareut/stock.adobe.com (passports). | GAO-25-107273

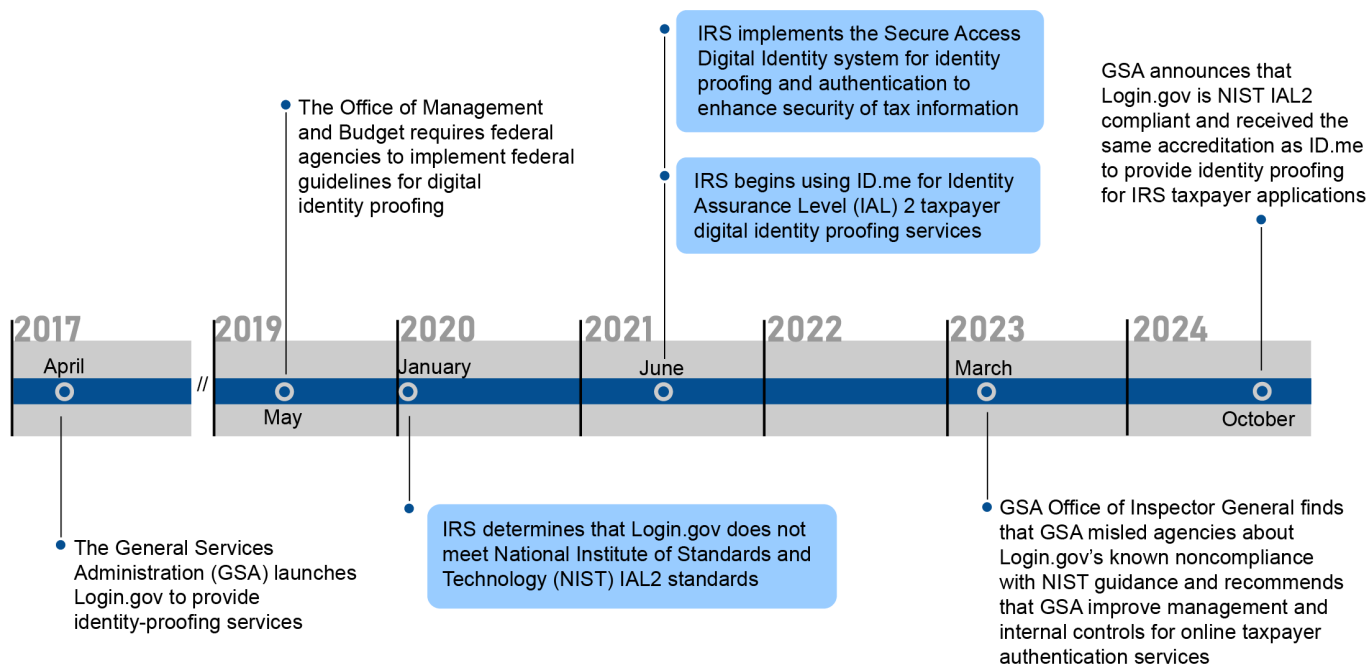
## Key Developments That Led to IRS's Current Digital Identity-Proofing Program

As of January 2025, IRS was using two CSPs—Login.gov and ID.me—to manage taxpayer access to more than 30 digital applications and services. See appendix II for a list of IAL1 and IAL2 digital applications. According to IRS officials, the agency does not use any IAL3 applications.

ID.me and Login.gov both handle interactions that require IAL1 credentials, such as trusted government-to-government information transactions, and instances requiring identity self-assertion. IRS also uses ID.me solutions to provide identity proofing for IAL2 secured applications such as accessing individuals' online accounts, reviewing prior year returns, and tracking refunds and payments, among other purposes. ID.me is currently IRS's only CSP for IAL2 applications. See appendix II for a full list of IRS's IAL1 and IAL2 online applications.

Figure 3 outlines key events that have led to changes in IRS identity proofing.

**Figure 3: Timeline of Key Taxpayer Identity-Proofing Events at the Internal Revenue Service (IRS)**



Source: GAO analysis of Treasury, IRS, and GSA information. | GAO-25-107273

In 2017, the General Services Administration (GSA) launched the Login.gov program.<sup>21</sup> Login.gov was intended to allow users access to multiple government agency programs securely and privately with one username and password. GSA reported that since its launch, Login.gov has been adopted by more than 40 federal and state agencies, and over 100 million users have signed up to use the system.

<sup>21</sup>The Consolidated Appropriations Act, 2016 required the Administrator of GSA to develop a single sign-on trusted identity platform. Per the act, the head of each agency, with exceptions, is required to implement the platform for individuals accessing each public website of the agency that requires user authentication. Pub. L. No. 114-113, div. N, § 225, 129 Stat. 2242, 2968 (2015), *codified at* 6 U.S.C. § 1523(b)(1)(D). Login.gov is maintained within GSA's Technology Transformation Services division.

---

In May 2019, OMB issued a memorandum that required federal agencies to implement NIST’s identity guidelines and any successive versions, which included the need for IAL2 capabilities for identity proofing.<sup>22</sup>

In January 2020, IRS determined that Login.gov did not include these services, so it had to find a different provider to meet the NIST standards. In July 2020, NIST released implementation guidance confirming the necessity of liveness detection, or biometric comparisons, for IAL2 remote identity proofing. In March 2023, GSA’s Office of Inspector General confirmed that Login.gov did not meet the IAL2 requirements and that GSA misled their customer agencies when GSA failed to communicate Login.gov’s known noncompliance with NIST guidance.<sup>23</sup>

In June 2021, IRS procured ID.me’s IAL2 online digital taxpayer identity-proofing solutions. According to IRS officials, the procurement was, in part, a response to NIST guidelines requiring the use of biometric data to confirm taxpayers’ identities and a law requiring IRS to set up the Advance Child Tax Credit portal.<sup>24</sup> Furthermore, at the time, ID.me was the only vendor with IAL 2 certification, which was required for certain IRS services, according to Treasury officials. The Treasury officials also said they conducted market research, gathered various mandates and requirements, and followed the GSA process to select the vendor.

The procurement coincided with IRS’s efforts to establish Secure Access Digital Identity (SADI) as its current identity-proofing program. After adopting SADI in June 2021, IRS stopped admitting new users to its legacy program, an in-house, knowledge-based identity-proofing approach that was decommissioned in June 2023.

SADI now uses third-party CSP solutions for identity proofing and authentication. This includes technology and support provided by ID.me to verify the identities of users for all IAL2 IRS applications and digital services. In May 2022, former IRS Commissioner Charles Rettig testified before the Senate Appropriations Subcommittee on Financial Services

---

<sup>22</sup>Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, M-19-17 (May 21, 2019).

<sup>23</sup>Office of Inspector General, U.S. General Services Administration, *GSA Misled Customers on Login.gov’s Compliance with Digital Identity Standards*, JE23-003 (Redacted) (Mar. 7, 2023).

<sup>24</sup>Pub. L. No. 117-2, § 9611(b), (c), 135 Stat. 4, 147, 150 (2021), *codified in part at* 26 U.S.C. § 7527A(c).

---

and General Government that ID.me’s authentication rate was about 70 percent compared to about 40 percent under the previous system.

In October 2024, GSA announced that Login.gov was certified and in compliance with IAL2 standards. At that time, IRS officials told us that they were developing plans to potentially use Login.gov for IAL2 applications.

Further, in October 2024, we reported that Login.gov provides benefits, but certain technical challenges were not being resolved in a timely fashion, potentially hindering its further adoption.<sup>25</sup> We made three recommendations to GSA to address NIST digital identity guidance and agency-identified technical issues and to document a plan for lessons learned for Login.gov’s remote identity-proofing pilot program.

---

## ID.me Contractual Arrangements

IRS uses ID.me solutions procured through a blanket purchase agreement (BPA) established by Treasury. In August 2020, Treasury established the BPA, and in June 2021, IRS began placing orders to obtain identity-proofing solutions in accordance with a Treasury directive.<sup>26</sup> IRS officials said that the BPA provided an appropriate mechanism for Treasury and its bureaus to procure ID.me solutions through V3Gate, a third-party software vendor that is also a veteran owned small business.<sup>27</sup> According to IRS officials, between June 2021 and April 2025, IRS obligated \$234.7 million for ID.me licenses and support services using the BPA.

Under the BPA, IRS awards delivery orders to V3Gate, as needed, to obtain identity-proofing solutions from ID.me. As the CSP of IAL2 services, the performance of ID.me’s solutions procured through V3Gate are critical to the goals of the program. In this report, we use the term “oversight” to refer to IRS’s internal control activities that include the

---

<sup>25</sup>[GAO-25-106640](#).

<sup>26</sup>Treasury encourages its bureaus to leverage shared services contracts and agreements to procure products and technology solutions such as ID.me identity proofing. Treasury Directive Publication TD P 81-01, *Treasury Information Technology Programs* (Oct. 20, 2022).

<sup>27</sup>Treasury established a BPA off a GSA-awarded schedule contract. The GSA federal supply schedule provides a simplified process for obtaining commercial supplies and services at prices associated with volume buying. Indefinite delivery contracts are awarded to provide supplies and services at stated prices for given periods of time. 48 C.F.R. § 8.402. Agencies using the schedules place orders or establish BPAs following established procedures. 48 C.F.R. § 8.405.



---

monitoring of the performance of the identity-proofing program and how it is being conducted, and not contractual oversight as defined by federal acquisition regulations.

In July 2021, IRS began using an additional contract vehicle to obtain fraud analytics through V3Gate and services provided by ID.me, such as support for fraud investigations, routine analysis of suspected fraudulent activity, and other risk assessments that go beyond what is available under the BPA. This procurement was through the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement. This government-wide acquisition contract provides IT, communication, and audio-visual products and services for any federal agency.<sup>28</sup> IRS requested these services to allow ID.me to share additional analysis and information to strengthen its efforts to track and combat fraud.

For example, under this contract ID.me assists IRS in identifying fraud schemes and provides an hourly report of fraudulent parties who successfully bypassed the ID.me identity-proofing process. IRS, V3Gate, and ID.me use these reports and fraud analytics to make improvements in identifying and combating fraudulent attempts to access IRS's digital applications. According to IRS officials, between August 2020 and August 2024, IRS obligated \$8.2 million to V3Gate for additional ID.me services using the government-wide acquisition contract.

---

<sup>28</sup>Government-wide acquisition contracts are multiple-award indefinite delivery, indefinite quantity contracts that allow government agencies to buy IT solutions and services directly from commercial providers. 40 U.S.C. § 11314(a)(2). Indefinite delivery, indefinite quantity contracts allow the government to order a stated minimum quantity of supplies or services, and the government may place orders to meet its needs during the ordering period. 48 C.F.R. § 16.504(c).

---

## IRS Has Taken Steps to Protect Users' Privacy and Monitors Aspects of ID.me's Performance, but Gaps Remain in Program Oversight

---

### IRS Has Taken Steps to Protect Users' Privacy

#### IRS Oversight of ID.me Fraud Detection Work

ID.me provides fraud data reporting under a separate contract than that for identity-proofing solutions. This contract, under the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement, includes a quality assurance surveillance plan that details required services, performance standards, methods of surveillance, and acceptable quality levels. Fraud data reports that are provided to IRS on a regular basis include

- information on accounts that have been suspended for suspected fraud, and
- information on accounts that have been suspended after taxpayers report they did not create the ID.me account.

ID.me officials said they systematically transmit information on account suspensions and reinstatements to IRS.

Source: GAO analysis of IRS and ID.me information. | GAO-25-107273

IRS established directives for ID.me solutions to protect users' privacy, which are included in delivery orders placed against the BPA.<sup>29</sup> The 12 directives which are intended to align with NIST standards include

- deletion of all biometric data within 24 to 48 hours for authenticated IRS online account credentials and user-abandoned IRS authentication attempts,
- deletion of all remote live chat session recordings within 30 calendar days, and
- provision of proof for IRS to confirm ID.me made the deletions.

IRS began including these directives in delivery order terms and conditions as part of several actions to address stakeholder and congressional concerns regarding the security and privacy of information

---

<sup>29</sup>We use BPA to refer to the Treasury BPA with V3Gate for ID.me identity-proofing solutions.

---

collected by ID.me.<sup>30</sup> For example, in February 2022, IRS and V3Gate modified their contract for identity proofing to add supervised remote sessions—these remote sessions allowed individuals to choose to verify their identities virtually with an ID.me agent, without needing to provide a selfie.

IRS also conducts and documents data validation checks on ID.me's solutions to ensure it is meeting the delivery order terms and conditions on an ongoing basis. For example, IRS inspected an ID.me facility in McLean, Virginia, where it reviewed code for deleting data. ID.me's solutions passed these reviews. IRS officials also said they compare ID.me usage data to IRS audit log data from SADI-protected systems on user access for validation. Officials also investigate ID.me-provided data to ensure their accuracy.

---

### IRS Works with V3Gate and ID.me to Monitor Identity-Proofing Solutions

The BPA also includes a statement of work listing various requirements relating to ID.me's performance, including the following:

- Holding a biweekly status call with government stakeholders to identify challenges, formulate action items, and discuss issues.
- Providing metrics on identity-proofing and authentication success and failures.
- Providing progress and performance reports using data elements to be determined by consultation between government stakeholders and the contractor.

The statement of work further stipulates that ID.me's solutions must undergo an independent quality assurance review which ensures compliance with NIST standards.<sup>31</sup> In addition, the first delivery order

---

<sup>30</sup>In January 2022, the Information Technology Acquisition Advisory Council—a nonprofit, public-private partnership that works with federal agencies to identify and meet IT modernization and cybersecurity challenges—sent a letter to IRS expressing concerns about privacy and security issues related to IRS's use of ID.me's solutions. Numerous members of Congress expressed their concerns with IRS's use of facial recognition technology to verify individuals' identities to access IRS's online services. ID.me officials told us that while the directives to protect users' privacy may have been well-intentioned, they were not backed by data and have resulted in a degraded fraud posture.

<sup>31</sup>The blanket purchase agreement requires the vendors to be certified by Kantara Initiative, a Federal Identity, Credential, and Access Management trust framework. Kantara Initiative is a 501(c)(6) nonprofit that provides standards for identity and personal data management. Kantara conducts independent assessments of CSPs' adherence to NIST standards on IAL 2 operation. Kantara lists ID.me as having been certified for following IAL 2 standards on its website. See <https://kantarainitiative.org/trust-status-list/> for more information.

---

issued against the BPA specifies that IRS is charged only for users whose identities are successfully proofed; according to V3Gate officials, this incentivizes performance and ensures the vendor is not paid for unsuccessful attempts.

IRS officials said they monitor the performance of ID.me solutions primarily through biweekly meetings and weekly progress and performance reports required in the BPA statement of work. IRS receives these reports through a computer dashboard interface provided by V3Gate and ID.me. The reports contain several measures, including how many users attempted identity proofing through ID.me, how many were successful, and how many were identified as having a high probability of being fraudulent (bad actors attempting to gain access to an IRS application).

The dashboard also contains a measure, the true pass rate, that tracks how many users successfully complete identity proofing compared to users who fail a step and do not continue the process. Other dashboard information includes which pathway the taxpayer used for identity proofing (e.g., self-service or video call) and the steps at which identity proofing failed. This includes steps such as how many users abandoned uploading a document, failed document verification, and abandoned providing a selfie. Additionally, the dashboard provides costs per user and time required for user identity proofing.

ID.me officials told us that they alert IRS when they see concerning patterns in user access data. They also said that ID.me has used its performance data to adjust how it operates. For example, ID.me officials said their reviews led them to develop additional support to help Puerto Rico residents successfully complete identity verification. ID.me officials said they have also worked to help provide additional support for people in the Mississippi Delta region without sufficient broadband internet access.

---

## IRS Used an Existing Agreement to Quickly Implement an Identity-Proofing Solution for the Advance Child Tax Credit Portal

When contracting for identity proofing, IRS followed Treasury's shared services-first policy to leverage the existing BPA, as described earlier. The policy is intended to shorten acquisition timelines, take advantage of competitive pricing, and achieve efficiencies in using the same provider across Treasury's bureaus and offices. According to IRS officials, the agency had to move quickly to launch the Advance Child Tax Credit portal, as required by the American Rescue Plan Act of 2021 in March

---

2021.<sup>32</sup> Officials said that leveraging the BPA allowed IRS to shorten the time needed to deploy identity proofing. This allowed IRS to meet Congress's mandate and launch a portal that enabled eligible taxpayers to register for the tax credit during the pandemic.

The BPA provided an acquisition vehicle for IRS to more quickly award a contract to V3Gate for ID.me solutions. IRS officials stated that ID.me also provided "heavy support" services to maintain the software, which are also provided for in the BPA. The BPA statement of work lists requirements for the software and for support services. Examples of the support services include database management, unlimited technical support, and unlimited call center support for all login and multifactor authentication help desk tickets. Our review of IRS documentation showed that IRS followed Federal Acquisition Regulation requirements to assess the quality, schedule, management, and regulatory compliance of the contractor's provision of the software and support services.

IRS officials said that because IRS is procuring ID.me software and support services from ID.me through a delivery order, they were not required to develop a performance assessment plan. This type of contract generally requires less stringent monitoring protocols than those required to oversee other types of contracts. In contrast, service contracts generally require the inclusion of a Quality Assurance Surveillance Plan, which would contain measurable inspection and acceptance criteria corresponding to any performance standards included in the contract.<sup>33</sup>

---

## IRS Oversight Weaknesses Limit IRS's Ability to Independently Manage Its Identity-Proofing Program

IRS needed to move quickly to make advance payments to eligible recipients of the Child Tax Credit during the pandemic, as previously discussed. IRS leveraged the BPA to help it move quickly, but as a result, gaps exist in how IRS manages its identity-proofing program. According to Treasury officials, the Treasury BPA is due to end in August 2025 and will be up for renewal. Officials said this milestone will provide IRS an opportunity to adjust its oversight and control activities to help ensure more robust management and evaluation of its identity-proofing program.

---

<sup>32</sup>IRS was required to establish the Advance Payment Program for the child tax credit, including establishing the portal, "as soon as practical" after the enactment of the American Rescue Plan Act of 2021. Pub. L. No. 117-2, § 9611(b), (c), 135 Stat. 4, 147, 150 (2021), *codified, in part, at* 26 U.S.C. § 7527A(c).

<sup>33</sup>48 C.F.R. § 46.401.

---

IRS officials acknowledge the program is a high-risk activity involving sensitive taxpayer data.

We found gaps in IRS's management in three general areas. First, IRS officials were unable to show us that they had independently documented measurable goals or objectives to manage the outcomes of its identity-proofing program. According to federal internal control standards, officials should define objectives clearly to enable the identification of risks and define risk tolerances.<sup>34</sup> Without independently established measures and goals, IRS cannot determine whether the performance of ID.me's solutions meets IRS needs.

Without goals or objectives set by IRS, it is also not clear which of the several measures that ID.me provides are the best matches for what IRS needs or what level of performance is appropriate for a given application. For example, ID.me's true pass rate excludes both users who abandon the process and users identified as highly probable fraudulent. In establishing measurable goals, IRS could determine that information on such users are essential performance measures that need to be established. Furthermore, as IRS continues to expand online services that require identity proofing it will need to consider additional metrics for these services.

Second, IRS officials were unable to show us that they evaluated or documented the outcomes of IRS's digital identity-proofing program, including ID.me solutions. According to federal internal control standards, officials should design control activities to achieve objectives and respond to risks.<sup>35</sup> While ID.me officials told us that they have used their own performance data to adjust how they operate, as discussed above, IRS officials were unable to demonstrate how they used any performance data to evaluate ID.me solutions. Without an evaluation plan with defined goals or objectives, IRS officials cannot independently or objectively evaluate how changes made by ID.me improve performance of its solutions involving taxpayer data; instead, they are relying on ID.me's own assessments of its solutions' performance. According to IRS, the contractual arrangement with ID.me does not require such a plan. Nevertheless, the inherent risk of identity proofing, the magnitude of services ID.me provides, and ID.me being IRS's sole provider of Identity

---

<sup>34</sup>See GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014). Principle 6.

<sup>35</sup>[GAO-14-704G](#), Principle 10.

---

Assurance Level (IAL) 2 identity-proofing solutions create a higher-risk environment for IRS management.

Third, IRS officials were unable to show us that they have documented procedures for sharing and communicating ID.me solutions' performance data to relevant IRS officials. Federal internal control standards state that management should communicate internally the necessary quality information to achieve the entity's objectives.<sup>36</sup> While ID.me shares its performance data through the V3Gate contract with potentially relevant staff within IRS, IRS officials could not explain how the data are shared or confirm that the recipients of the data are the relevant reviewers in IRS. Without documented procedures for sharing and communicating ID.me solutions' performance data, relevant IRS officials cannot have assurance they are consistently receiving the data they need to make informed determinations about IRS's identity-proofing program, potentially hindering their ability to take appropriate corrective actions.

---

### IRS Has Not Taken Steps to Comply with AI Oversight Requirements for ID.me

ID.me's identity-proofing solution uses AI technologies, including facial-recognition technology. However, as of March 2025, IRS has not documented these uses in its AI inventory. As a result of not including ID.me's AI technologies in its inventory, IRS has not taken steps to comply with IRS's own AI oversight requirements.

Executive Order 13960 and the Advancing American AI Act require most agencies to document AI, including contracted AI, in a central agency inventory.<sup>37</sup> In May 2024, IRS published an AI governance policy that formalized the agency's inventory requirements and an oversight process for AI, including contracted AI.<sup>38</sup> In March 2025, IRS updated its internal

---

<sup>36</sup>GAO-14-704G, Principle 14.

<sup>37</sup>Exec. Order No. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 85 Fed. Reg. 78939 (Dec. 8, 2020); James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, §§7221-7228, 136 Stat. 3668-3676 (2022) (*reprinted* in 40 U.S.C. § 11301 note).

<sup>38</sup>IRS Interim Guidance Memorandum (RAAS-10-0524-0001), Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles (May 20, 2024).

---

guidance to reflect changes in federal requirements.<sup>39</sup> IRS's updated guidance maintains its requirements for an internal inventory of AI and other documentation requirements.

Specifically, IRS's policy aims to ensure its use of AI complies with government-wide and agency requirements. Principles established in EO 13960 and adopted in IRS policy include, among others, ensuring that the use of AI protects taxpayer's rights and is accurate, reliable, effective, and transparent. To comply with IRS's documentation requirements, those responsible for the AI—including contractors—provide information including a summary detailing the intended application of the AI, the data used to develop the AI, its limitations, and performance metrics. Collectively, this required documentation can help promote transparency on how AI is being used by IRS and its intended outcomes.

According to the ID.me website, ID.me uses AI—including facial recognition technology—to complete parts of the identity-proofing process. For example, ID.me AI compares an online user's image to photos on official documents to authenticate a taxpayer's identity. IRS officials responsible for AI oversight said ID.me's use of AI was likely subject to AI oversight requirements. However, an IRS official responsible for working with ID.me on its identity-proofing solution stated he was not aware that ID.me's identity-proofing solutions should be subject to IRS's AI oversight requirements. According to IRS's AI oversight officials, as of March 2025, they had met with those working with ID.me on identity proofing to discuss including ID.me in IRS's AI inventory, but they had not added ID.me AI to the inventory or completed other documentation requirements.

By not documenting ID.me's use of AI in IRS's AI inventory, IRS cannot ensure that ID.me's identity-proofing solutions comply with agency

---

<sup>39</sup>IRS's May 2024 guidance was based in part on Executive Order 14110, which was rescinded in January 2025. In March 2025, IRS issued an updated interim policy for AI Governance which superseded the May 2024 guidance. For more detail, see IRS Interim Guidance Memorandum (RAAS-10-0325-0001), Interim Policy for AI Governance (Mar. 11, 2025); Exec. Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed. Reg. 75191 (Nov. 1, 2023); Exec. Order No. 14148 *Initial Rescissions of Harmful Executive Orders and Actions*, 90 Fed. Reg. 8237 (Jan. 28, 2025); Exec. Order No. 14179 *Removing Barriers to American Leadership in Artificial Intelligence*, 90 Fed. Reg. 8741 (Jan. 31, 2025). In response to requirements in Executive Order No. 14179, OMB published revised memos in April 2025 which fall outside the scope of this engagement. See OMB M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* (Apr. 3, 2025); OMB M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (Apr. 3, 2025).



---

requirements or reflect the government-wide principles for AI use. Stronger oversight of IRS's use of AI-enabled solutions would better position IRS to ensure taxpayers' rights are protected and the technology is accurate, reliable, effective, and transparent.

---

## Conclusions

All of IRS's most sensitive identity-proofing activities—IAL2 solutions—are currently built upon a single CSP, ID.me. Implementing and maintaining robust oversight of its vendor's identity-proofing solutions is integral to IRS effectively managing its digital identity-proofing program and thus critical for maintaining public trust of our tax system and for encouraging taxpayers to use online services.

IRS has taken several steps to ensure that ID.me protects users' privacy. For example, ID.me provides IRS with data on its identity-proofing solutions, and IRS checks to ensure ID.me privacy protections are in place and that data it uses are valid.

However, gaps exist in IRS's oversight of its digital identity-proofing program. IRS has not demonstrated that it has documented performance goals and objectives for the program or an independent method for evaluating its outcomes. IRS also has not shown that it has documented procedures to share ID.me performance data with relevant officials. Taking action to close these gaps would help ensure IRS's identity-proofing program is progressing toward IRS's desired outcomes. Finally, IRS has not included ID.me on its inventory of programs using AI, limiting IRS's assurance that procurements using AI are used in alignment with IRS policy so that taxpayers' rights are protected and the technology is accurate, reliable, effective, and transparent.

## Recommendations for Executive Action

We are making the following four recommendations to IRS:

The Commissioner of Internal Revenue should define and document measurable goals and objectives for its digital identity-proofing program. (Recommendation 1)

The Commissioner of Internal Revenue should regularly evaluate and document results of its digital identity-proofing program in terms of meeting the goals and objectives established in recommendation 1. (Recommendation 2)

The Commissioner of Internal Revenue should establish procedures for routinely sharing and communicating identity-proofing vendors' performance data to relevant officials. (Recommendation 3)

---

The Commissioner of Internal Revenue should ensure that procured digital identity-proofing solutions that involve the use of AI are included in IRS's AI inventory, consistent with applicable legal requirements, and go through IRS's AI oversight process. (Recommendation 4)

---

## Agency Comments

We provided a draft of this report to the Commissioner of Internal Revenue for comment. In its written comments, reproduced in appendix III, IRS agreed with our four recommendations and said they would fully implement them. IRS and ID.me also provided technical comments, which we incorporated as appropriate.

---

We are sending copies of this report to the Commissioner of Internal Revenue, the appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at [mctiguej@gao.gov](mailto:mctiguej@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

**//SIGNED//**

James R. McTigue, Jr.  
Director, Strategic Issues  
Tax Policy and Administration

---

# Appendix I: Objectives, Scope, and Methodology

---

To address how the Internal Revenue Service (IRS) manages its identity-proofing program, including ID.me solutions' identity-proofing performance, as well as ID.me's use of artificial intelligence (AI), we reviewed documentation on federal guidelines and IRS policies related to identity proofing, including relevant National Institute of Standards and Technology standards, Internal Revenue Manual policies governing identity verification and authentication processes, and IRS's identity-proofing security plans. We focused on IRS's identity assurance level 2 (IAL2) activities, all of which involve products and support services provided by ID.me. We interviewed relevant IRS officials and ID.me staff about ID.me's identity-proofing procedures and how V3Gate and ID.me work with IRS.

To collect information on ID.me solutions' reported performance, we reviewed ID.me data and ID.me-related contract documentation. The performance data we reviewed included monthly and annual ID.me performance reports submitted by V3Gate, IAL2 digital applications usage data, fraud analytics, and feedback from knowledgeable stakeholder groups. Contracting documentation we reviewed included a blanket purchase agreement (BPA), statements of work, contract modifications, a performance work statement, a quality assurance surveillance plan, contract performance assessment reports, ID.me's records deletion report, IRS's attestation of digital identity risk assessments, delivery and task orders, and related documentation. We also interviewed relevant contracting officials with the Department of the Treasury, IRS, V3Gate, and ID.me. We collected documentation on activities that IRS conducts to monitor ID.me.

To calculate the amount of funding devoted to ID.me, we reviewed Treasury BPA orders, including modifications, and orders placed against a government-wide acquisition vehicle. We collected and analyzed funding data for each order issued between September 2020 and August 2024 from the Federal Procurement Data System, and validated and confirmed our results.

We compared the documentation and interviews we compiled on IRS's ID.me monitoring activities to relevant federal internal control standards—specifically, internal control standards for defining objectives, designing

control activities, and communicating internally.<sup>1</sup> We also reviewed ID.me's public documentation and met with officials knowledgeable about IRS's identity-proofing contracts and AI oversight requirements. We also reviewed relevant federal laws and guidance, IRS oversight policies related to AI, and IRS's AI inventory.

We assessed the reliability of ID.me and IRS performance and contract data by reviewing documents, discussing data reliability methods used with those responsible, and examining the data for internal consistency or anomalies. We found the data to be reliable for the purpose of analyzing ID.me performance, reviewing IRS monitoring efforts, and determining total obligations for ID.me identity-proofing solutions.

To better understand identity-proofing issues, we conducted semi-structured interviews with knowledgeable federal and non-federal stakeholders about related programs, services, and technology. To select the interviewees, we performed a literature search for relevant publications, reviewed our prior relevant work, and asked stakeholders whom we spoke with for referrals to others who could provide additional perspectives.

For additional background and context, we reviewed academic literature, government reports, and industry white papers, among other sources, to identify articles discussing what is known about taxpayer identity proofing. For our literature search, we considered publications from 2019 to 2024 that studied or commented on IRS's authentication programs and services, or the technology used by ID.me in conducting identity proofing as a credential services provider for IRS. We considered and reviewed sources' websites for obvious bias or lack of fit for the subject. We reviewed the literature search results and identified the most relevant reports given our engagement scope and objectives.

We conducted our work from February 2024 to June 2025 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 objectives. We believe that the evidence obtained

---

<sup>1</sup>See GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014). Internal control is a process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

---

**Appendix I: Objectives, Scope, and  
Methodology**

---

provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: IRS Applications Requiring Identity Proofing

As of January 2025, the Internal Revenue Service (IRS) was using two credential service providers—Login.gov and ID.me—to allow taxpayers to access more than 30 online applications.

ID.me and Login.gov both handle interactions that require what the National Institute of Standards and Technology defines as identity assurance level (IAL) 1 identity-proofing credentials. IAL1 credentials are intended for lower-risk transactions and applications requiring identity self-assertion. For IAL2 applications, at a minimum, the individual will need a computer or mobile phone that has a camera, an email address, and a valid government-issued photo ID, among other sources of information.

IRS has an agreement with IT solutions reseller V3Gate for ID.me to provide both IAL1 and IAL2 identity proofing for IRS’s public-facing applications, such as accessing individual online accounts, submitting tax returns, reviewing prior year returns, and tracking refunds and payments. Table 2 provides a list of IAL-secured IRS online applications. In some cases, the user has the option to use Login.gov or ID.me.

**Table 2: Internal Revenue Service Applications Requiring Identity Assurance Level (IAL) 1 and 2 Identity Proofing**

Application	IAL	Credential service provider
Affordable Care Act - Information Submission Services - User Interface	IAL2	ID.me
Affordable Care Act - Information Submission Services - User Interface – Assurance Testing System	IAL2	ID.me
Automated Enrollment Affordable Care Act Transmitter Control Code & Services	IAL2	ID.me
Automated Lien System - Extranet	IAL1	Login.gov or ID.me
Business Tax Accounts	IAL2	ID.me
Clean Energy	IAL2	ID.me
Direct File	IAL2	ID.me
eGain - ACS Authenticated Web Chat	IAL2	ID.me
eGain - Appeals	IAL2	ID.me
eGain - Secure Messaging	IAL2	ID.me
ePostcard	IAL1	Login.gov or ID.me
Electronic Services Consent Application Programming Interface	IAL2	ID.me
Electronic Services External Services Authorization Management	IAL2	ID.me
Electronic Services Partnership Bipartisan Budget Act - Electronic Forms Submission	IAL2	ID.me
Electronic Services Secure Object Repository	IAL2	ID.me
Electronic Services Transcript Delivery System	IAL2	ID.me

**Appendix II: IRS Applications Requiring  
Identity Proofing**

<b>Application</b>	<b>IAL</b>	<b>Credential service provider</b>
Electronic Services Taxpayer Identification Number Matching	IAL2	ID.me
Electronic Services Terms of Service	IAL2	ID.me
Foreign Account Tax Compliance Act Financial Institution – Registration	IAL1	Login.gov or ID.me
Foreign Account Tax Compliance Act Qualified Intermediary	IAL1	Login.gov or ID.me
Individual Online Account	IAL2	ID.me
Information Returns Intake System 1099 Portal	IAL2	ID.me
Income Verification Express Service Form Based Process	IAL2	ID.me
Kiteworks	IAL2	ID.me
Modernized Electronic Filing - Internet Filing Application - Assurance Testing System	IAL2	ID.me
Modernized Electronic Filing - Internet Filing Application - Production	IAL2	ID.me
Online Payment Agreement - Business Masterfile	IAL2	ID.me
Online Payment Agreement - Individual Masterfile	IAL2	ID.me
Online Payment Agreement - Individual	IAL2	ID.me
Tax Professional Account	IAL2	ID.me
Taxpayer Digital Communications - Form 2848 & Form 8821 Intake	IAL2	ID.me
Taxpayer Protection Program Identity and Tax Return Verification Service	IAL2	ID.me
Task, Request, and Case Management System	IAL2	ID.me

Source: GAO review of IRS information. | GAO-25-107273

# Appendix III: Comments from the Internal Revenue Service



DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, DC 20224

May 13, 2025

Mr. James R. McTigue, Jr.  
Director, Tax Policy and Administration  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548

Dear Mr. McTigue:

Thank you for providing the GAO-25-107273 draft report "Tax Identity Verification: IRS Should Expeditiously Strengthen Oversight of Its Identity-Proofing Program" (JC#107273)" and allowing the IRS and the Department of the Treasury (Treasury) to review and respond to the draft. In this letter, I am responding on behalf of both the IRS and Treasury.

Your report assessed how IRS monitors and oversees the performance of its digital identity-proofing program, which is a critical enabler for modernization efforts to expand digital service offerings.

In June 2021, the IRS accelerated the launch of the digital identity platform in response to federal mandates (e.g., American Rescue Plan Act, Creating Advanced Streamlined Electronic Services for Constituents Act, National Institute of Standards and Technology, Special Publication 800-63-3, and Office of Management and Budget Memo 19-17) and to drive more taxpayers to the digital channel through an improved user experience and strengthened security to protect taxpayer data.

The digital identity platform allows taxpayers to securely access IRS resources online in compliance with federal guidelines, while reducing burdens on non-digital channels and service costs to the IRS. This program is designed to reach taxpayer populations that have traditionally struggled to identity proof with the IRS. This includes underbanked populations, those with little to no credit history, and first-time filers.

The IRS introduced a federated approach to digital identity using a Credential Service Provider, which allows taxpayers to access online applications across different government agencies using a single set of credentials. The IRS currently uses ID.me for identity verification and credential management services for access to IRS online applications that require Identity Assurance Level 2. Additionally, IRS offers both Login.gov and ID.me certain IRS online applications that only require self-assertion at Identity Assurance Level 1.

To meet the accelerated deployment timeframe for this digital identity solution, the IRS leveraged the Treasury Blanket Purchase Agreement to acquire ID.me identity verification licenses and associated products support through various delivery orders.



---

**Appendix III: Comments from the Internal  
Revenue Service**

---

2


Due to the nature of the products contract vehicles, a quality assurance surveillance plan was not required nor completed to define performance measures for the IRS's digital identity verification program.

We appreciate the valuable feedback that you provided in your report to address documentation and procedural gaps for defining program objectives, evaluation of results, and communicating vendor performance metrics with business unit officials. The IRS agrees with the recommendations, which will be fully implemented.

Again, thank you for providing the report and valuable feedback. We provided technical comments on the draft separately. If you have questions, please contact me, or a member of your staff may contact John Lyons, Director of Identity Assurance at 267-466-2053.

Sincerely,

Dottie A.  
Romo

 Digitally signed by Dottie  
A. Romo  
Date: 2025.05.13  
07:17:17 -0400

Dottie Romo  
Acting Chief Operating Officer

Enclosure

---

# Appendix IV: GAO Contact and Staff Acknowledgments

---

## GAO Contact

James R. McTigue, Jr., [mctiguej@gao.gov](mailto:mctiguej@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, Jessica Nierenberg (Assistant Director), Eric Gorman (Analyst-in-Charge), Peter Beck and Jesse Mitchell made key contributions to this report. Also contributing to this report were Pille Anvelt, Jennifer Dougherty, Robert Gebhart, Gina Hoover, Christine Pecora, Ethan Pham, Emily D. Smith, Andrew J. Stephens, Nathan Tranquilli, Robyn Trotter, Mercedes Wilson-Barthes, and Melanie Magnotto Win.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).  
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

---

## Media Relations

Sarah Kaczmarek, Managing Director, [Media@gao.gov](mailto:Media@gao.gov)

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [CongRel@gao.gov](mailto:CongRel@gao.gov)

---

## General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.