



June 2018

# IDENTITY THEFT

## IRS Needs to Strengthen Taxpayer Authentication Efforts

# GAO Highlights

Highlights of [GAO-18-418](#), a report to congressional requesters

## Why GAO Did This Study

Strong preventive controls can help IRS defend itself against identity theft refund fraud. These controls include taxpayer authentication—the process by which IRS verifies identities before allowing people access to a resource; sensitive data; or, in some cases, a tax refund. The risk of fraud has increased as more personally identifiable information has become available as a result of, for example, large-scale cyberattacks on various entities. IRS’s ability to continuously monitor and improve taxpayer authentication is a critical step in protecting billions of dollars from fraudsters.

GAO was asked to examine IRS’s efforts to authenticate taxpayers. This report (1) describes the taxpayer interactions that require authentication and IRS’s methods; (2) assesses what IRS is doing to monitor and improve taxpayer authentication; and (3) determines what else, if anything, IRS can do to strengthen taxpayer authentication in the future.

To meet these objectives, GAO reviewed IRS documents and data, evaluated IRS processes against relevant federal internal control standards and guidance, and interviewed IRS officials and state and industry representatives.

## What GAO Recommends

GAO is making 11 recommendations to IRS to estimate resources for and prioritize its authentication initiatives, address internal control issues to better monitor authentication, develop a plan to fully implement new NIST guidance, and develop a process to evaluate potential authentication technologies. IRS agreed with GAO’s recommendations.

View [GAO-18-418](#). For more information, contact James R. McTigue, Jr. at (202) 512-9110 or [mctiguej@gao.gov](mailto:mctiguej@gao.gov)

June 2018

## IDENTITY THEFT

### IRS Needs to Strengthen Taxpayer Authentication Efforts

## What GAO Found

The Internal Revenue Service (IRS) has identified over 100 interactions requiring taxpayer authentication based on potential risks to IRS and individuals. IRS authenticates millions of taxpayers each year via telephone, online, in person, and correspondence to ensure that it is interacting with legitimate taxpayers. IRS’s estimated costs to authenticate taxpayers vary by channel.

**Taxpayers Authenticated for Selected IRS Programs, 2017**

IRS Taxpayer Authentication by Channel				
	Telephone Service	Online Service	In-person Service	Correspondence Service
<b>Taxpayers Authenticated</b>	7,211,600	16,502,000	945,100	3,941,700
<b>Estimated Cost Per Interaction</b>	60 cents (automated) to \$54 (live assistor)	20 cents	\$89	60 cents (mailing) to \$65 (document review)

Source: GAO analysis of Internal Revenue Service (IRS) documents and data. | GAO-18-418

Notes: Numbers are rounded to the nearest hundred and represent successful authentications. Cost information is rounded to the nearest dollar unless otherwise noted. Data are for IRS’s Taxpayer Protection Program, Get Transcript, Identity Protection Personal Identification Number, and taxpayer online accounts.

IRS has made progress on monitoring and improving authentication, including developing an authentication strategy with high-level strategic efforts. However, it has not prioritized the initiatives supporting its strategy nor identified the resources required to complete them, consistent with program management leading practices. Doing so would help IRS clarify relationships between its authentication efforts and articulate resource needs relative to expected benefits. Further, while IRS regularly assesses risks to and monitors its online authentication applications, it has not established equally rigorous internal controls for its telephone, in-person, and correspondence channels, including mechanisms to collect reliable, useful data to monitor authentication outcomes. As a result, IRS may not identify current or emerging threats to the tax system.

IRS can further strengthen authentication to stay ahead of fraudsters. While IRS has taken preliminary steps to implement National Institute of Standards and Technology’s (NIST) new guidance for secure digital authentication, it does not have clear plans and timelines to fully implement it by June 2018, as required by the Office of Management and Budget. As a result, IRS may not be positioned to address its most vulnerable authentication areas in a timely manner. Further, IRS lacks a comprehensive process to evaluate potential new authentication technologies. Industry representatives, financial institutions, and government officials told GAO that the best authentication approach relies on multiple strategies and sources of information, while giving taxpayers options for actively protecting their identity. Evaluating alternatives for taxpayer authentication will help IRS avoid missing opportunities for improving authentication.

---

# Contents

---

---

Letter		1
	Background	5
	IRS Incorporates Risk and Other Factors to Guide Authentication Decisions for Taxpayer Interactions	10
	IRS Has Made Progress on Its Authentication Efforts, but Has Not Prioritized Authentication Improvements and Is Not Sufficiently Assessing and Monitoring Risks for Telephone and In-Person Authentication	16
	IRS Has Improved Its Authentication Methods, but Additional Actions Could Help Enhance Security	30
	Conclusions	41
	Recommendations for Executive Action	43
	Agency Comments and Our Evaluation	44
Appendix I	Objectives, Scope, and Methodology	47
Appendix II	Overview of IRS's Identity Assurance Strategy and Roadmap	52
Appendix III	Comments from the Internal Revenue Service	54
Appendix IV	GAO Contact and Acknowledgments	59
Related GAO Products		60
Table		
	Table 1: Overview of the Internal Revenue Service's (IRS) Identity Assurance Strategy and Roadmap	52
Figures		
	Figure 1: IRS Authentication Channels and Associated Costs (Based on Fiscal Year 2017 Data)	13

---

---

Figure 2: Usage and Costs of Selected IRS Programs and Services That Require Authentication, 2017	15
Figure 3: Example of a Federated Model for Authentication	37
Figure 4: Authentication Process Using Universal Authentication Framework and Universal Second Factor	39

---

---

## Abbreviations

AMS	Account Management Services
CSR	customer service representative
e-authentication	electronic authentication
e-file	electronically file
FAFSA	Free Application for Federal Student Aid
FIDO Alliance	Fast Identity Online Alliance
GSA	General Services Administration
IAO	Identity Assurance Office
IDT	identity theft
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
RAAS	Office of Research, Applied Analytics, and Statistics
RICS	Return Integrity and Compliance Services
<i>Roadmap</i>	<i>IRS Identity Assurance Strategy and Roadmap</i>
SSA	Social Security Administration
SSN	Social Security number
<i>Strategic Plan</i>	<i>IRS Strategic Plan, Fiscal Years 2014-2017</i>
<i>Taxonomy</i>	<i>IRS Identity Theft Taxonomy</i>
TIGTA	Treasury Inspector General for Tax Administration
TPP	Taxpayer Protection Program
UAF	Universal Authentication Framework
U2F	Universal Second Factor
VA	Department of Veterans Affairs
W-2	<i>Form W-2, Wage and Tax Statements</i>

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 22, 2018

Congressional Requesters

Our prior work has found that strong preventive controls can help the Internal Revenue Service (IRS) defend itself against tax fraud.<sup>1</sup> These controls include taxpayer authentication—in general, the process by which IRS verifies people’s identities before allowing them access to sensitive data (such as tax return information from a prior year) or, in the case of a suspicious tax return, a refund. IRS also uses authentication to verify a person’s identity before allowing access to a resource, such as an information technology (IT) system.

The risk of fraud has increased as more personally identifiable information (PII) has become readily available as a result of, for example, large-scale cyberattacks on entities including IRS, the Office of Personnel Management (OPM), and, recently, Equifax.<sup>2</sup> In May 2015, IRS temporarily suspended its Get Transcript service after fraudsters used personal information obtained from sources outside IRS to pose as legitimate taxpayers and access tax return information from up to 724,000 accounts.<sup>3</sup> In June and July 2015, OPM announced two data breaches affecting approximately 22.1 million current or former federal employees and contractors and their family members. Among the data stolen were Social Security numbers (SSN) and financial and personal health information. In September 2017, Equifax announced that criminals had

---

<sup>1</sup>We have found that implementing such controls can generally help protect IRS against the difficulties of trying to recover a fraudulent refund once issued. Recapturing a fraudulent refund after it is issued can be challenging—if not impossible—because identity thieves often spend or transfer the funds immediately, making them very difficult to trace. See GAO, *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>2</sup>Equifax is one of the three largest nationwide credit bureaus that provide lenders, employers, and other entities with reports that are commonly used to determine eligibility for credit, employment, and insurance. Equifax also provides services to organizations including income and employment verification, risk-based authentication tools, and identity validation.

<sup>3</sup>IRS suspended the Get Transcript service from May 2015 to June 2016. The Get Transcript service provides users, via the IRS website, the ability to view, print, and download tax account, tax return, and record of account transcripts; wage and income documents; and proof of nonfiling transcripts. Taxpayers can also obtain transcripts by calling, writing, or walking into an IRS office.

---

exploited a vulnerability in its systems and obtained PII on 145.5 million individuals including names, SSNs, birth dates, addresses, and in some cases, driver's license information. In March 2018, Equifax announced, after further investigation, that criminals stole partial driver's license information for an additional 2.4 million individuals. The proliferation of stolen PII poses a threat to the tax system by making it difficult for IRS to distinguish legitimate taxpayers from fraudsters. This threat is particularly acute during the filing season when IRS and taxpayers interact the most.

IRS estimates that at least \$12.2 billion in identity theft (IDT) tax refund fraud was attempted in calendar year 2016, and that it prevented the theft of at least \$10.5 billion of that amount. However, IRS reports that at least \$1.6 billion was paid out to fraudsters.<sup>4</sup> IRS's ability to continuously monitor and improve its approach to taxpayer authentication is a critical step in defending the agency against evolving cyber threats and fraud schemes and in protecting billions of taxpayer dollars. To further address IDT refund fraud, IRS held a Security Summit in March 2015 with state tax administrators and industry partners, including tax preparation and software firms and financial institutions. This ongoing effort is intended to improve information sharing and collaboratively address critical issues, including authentication and fraud detection.

Within this context, you asked us to examine IRS's efforts to authenticate taxpayers. This report (1) describes the taxpayer interactions that require authentication, including the general rationale behind the requirements, and IRS's authentication methods; (2) assesses what IRS is doing to monitor and improve its authentication methods, both internally and collaboratively through the Security Summit, to secure taxpayer information and reduce IDT refund fraud; and (3) determines what else, if anything, IRS can do to strengthen its authentication methods while improving services to taxpayers in the future.

---

<sup>4</sup>IRS's *Identity Theft Taxonomy (Taxonomy)* estimates the number and cost of identified IDT refund fraud cases where (1) IRS prevented or recovered the fraudulent refunds and (2) paid the fraudulent refunds. In November 2017, IRS noted that because of changes in its fraud detection and calculation methodology for the 2016 Taxonomy, results are not fully comparable to prior year data. Nevertheless, the agency reports that the 2016 estimates indicate an overall decline in identity theft attempts. However, because of the difficulties in estimating the amount of undetectable fraud, the actual amount could differ from these estimates. Also see GAO, *Identity Theft and Tax Fraud: IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, [GAO-16-508](#) (Washington, D.C.: May 24, 2016).

---

To describe the interactions that require taxpayer authentication and IRS's authentication methods, we reviewed IRS documents, policies and procedures, and IRS-reported information related to taxpayer authentication volume and costs per transaction for fiscal years 2016 and 2017. We determined that the data were sufficiently reliable for our purposes. We also interviewed IRS officials knowledgeable about the agency's authentication programs and services offered to taxpayers through various channels. For this report, we focused on the following four IRS programs and services because they require taxpayer authentication, verify a significant number of taxpayer identities each year, and illustrate IRS's different approaches to authentication:

- the Taxpayer Protection Program (TPP),
- Get Transcript,
- Identity Protection Personal Identification Number (IP PIN), and
- IRS's online services.

To assess IRS's efforts to monitor and improve authentication internally and through the Security Summit, we reviewed IRS policies, procedures, authentication risk assessments, and information on authentication performance. To better understand IRS's efforts to authenticate taxpayers via telephone and in-person and how customer service representatives (CSR) record data for authentication, we selected a random, generalizable sample of records from IRS's Account Management Services (AMS) to create estimates about IRS's authentication outcome data for TPP. We determined that these data were sufficiently reliable for the purpose of our review based on discussions with knowledgeable IRS officials and by checking key data elements for out-of-range or logically inaccurate data. (See appendix I for more information.) We also compared IRS's efforts to applicable activities in the *IRS Identity Assurance Strategy and Roadmap (Roadmap)*, *IRS's Strategic Plan Fiscal Years 2014-2017 (Strategic Plan)*, *Standards for Internal Control in the Federal Government*, *GAO's Framework for Managing Fraud Risks in Federal Programs*, and relevant National Institute of Standards and Technology (NIST) guidance.

We interviewed IRS officials in Return Integrity and Compliance Services (RICS), Identity Assurance Office (IAO), and IT knowledgeable about the agency's taxpayer authentication programs. We also interviewed IRS, state, and industry co-leads from two Security Summit workgroups to understand IRS's collaborative efforts to improve taxpayer authentication.



---

To evaluate what else, if anything, IRS can do to strengthen its authentication methods while improving services to taxpayers, we interviewed IRS officials knowledgeable about the agency's plans for taxpayer authentication. We also met with officials from the General Services Administration (GSA) who are developing a government-wide authentication platform; officials from the Office of Management and Budget (OMB) who were involved in developing IRS's Secure Access platform; and officials from the Department of Veterans Affairs (VA) who are working with a third-party identity proofing service to authenticate veterans applying for benefits online. Further, we met with knowledgeable officials from the National Institute of Standards and Technology (NIST) to discuss its guidelines for online identity-proofing and authentication.<sup>5</sup> Based on referrals from NIST and Security Summit workgroup co-leads and our prior work in this area, we also interviewed a nongeneralizable selection of representatives from state revenue offices, industry, and financial institutions. In total, we met with representatives from five state departments of revenue and one association representing state tax officials, three financial institution organizations, one financial service industry association, three identity-proofing/authentication organizations, and four tax industry organizations. We compared IRS's authentication programs and plans for future improvements to its *Strategic Plan and Roadmap*, federal internal controls, guidance from NIST and OMB, principles for project planning, our prior work on the Government Performance and Results Act, our *Information Technology Investment Management framework*, and our *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*.<sup>6</sup> For a more detailed description of our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from January 2017 to June 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

---

<sup>5</sup>National Institute of Standards and Technology, *Electronic Authentication Guideline, Special Publication 800-63-2*, (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).

<sup>6</sup>GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004); and *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).

---

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 our findings and conclusions based on our audit objectives.

---

## Background

---

### Authentication Provides IRS Reasonable Assurance That It Is Interacting with Legitimate Taxpayers

IRS authenticates taxpayers to provide the agency with reasonable assurance that it is interacting with the legitimate taxpayer. IRS verifies that it is interacting with the legitimate taxpayer through identity proofing and authentication. Identity proofing is the process of first establishing that people are actually who they claim to be. Authentication is the process of verifying that returning users are who they say they are by requiring the use of one or more authenticators—such as a password, a cryptographic key, or a fingerprint—before allowing them access to sensitive data or a resource. In this report, we refer to both steps collectively as “authentication.”

For high-risk interactions, such as access to prior year tax information, authentication can help IRS avoid improperly disclosing PII or issuing a fraudulent refund. Authentication is particularly important for combatting IDT refund fraud, which occurs when a fraudster obtains an individual’s SSN, date of birth, or other PII and uses it to file a fraudulent tax return seeking a refund. IDT refund fraud can also affect businesses. Specifically, fraudsters can use business information to file a fraudulent corporate return requesting a refund. According to IRS officials, fraudsters can file false employer *Form W-2, Wage and Tax Statements (W-2)* to support fraudulent individual returns seeking refunds. We have previously reported that when IRS suspects that a tax return is fraudulent, it will stop the return from further processing, and attempt to notify and authenticate the taxpayer before issuing the refund.<sup>7</sup>

Authentication can be accomplished using different methods depending on the risk of the interaction.

---

<sup>7</sup>See [GAO-16-508](#) for more information.

- 
- **Single-factor authentication:** Useful when someone wants to access a low-risk system or service, this method may require only a user name and password.
  - **Multi-factor authentication:** For high-risk interactions such as access to systems that include PII or financial information, this method requires at least two of the following: “something you know” (e.g., a user name and password); “something you have” (e.g., a mobile phone or cryptographic key); or “something you are” (e.g., a fingerprint or other biometric data).

Designing authentication programs involves a balancing act—IRS needs to prevent fraudsters from passing authentication using stolen taxpayer information, but it must balance that against the burden on legitimate taxpayers who must also authenticate. If IRS makes the authentication process too stringent, legitimate taxpayers may not be able to successfully authenticate to, for example, access their prior year tax information or have IRS release a frozen refund. Conversely, if the process is too easy, fraudsters will likely be able to authenticate as easily as legitimate taxpayers.

Industry representatives told us that identity proofing and authentication are becoming more difficult with the wide availability of PII. Further, according to NIST, it is challenging for organizations to authenticate users remotely via a web application because the processes and technologies to establish and use digital identities offer multiple opportunities for impersonation or other attacks. These interactions may become even more difficult and risky for organizations like IRS, who may interact with a taxpayer only once a year.

As shown by the data breaches discussed at the beginning of this report, fraudsters are persistent in their efforts to exploit weaknesses in online systems and, in the context of IRS, access sensitive taxpayer information. For example, IRS reported that, between January and March 2017, fraudsters were able to use PII to access information from 100,000 taxpayer accounts through IRS’s Data Retrieval Tool.<sup>8</sup> According to the Treasury Inspector General for Tax Administration, identity thieves may have used PII obtained outside the tax system to start the Free

---

<sup>8</sup>IRS’s Data Retrieval Tool allowed students and parents to access and transfer their tax information from IRS while completing the Department of Education’s FAFSA. According to IRS officials, after identifying anomalies with the use of the Data Retrieval Tool, IRS worked with the Department of Education to update the Data Retrieval Tool and FAFSA applications to prevent inappropriate access to tax data.

---

Application for Federal Student Aid (FAFSA) application process and access tax information through the Data Retrieval Tool.<sup>9</sup> Further, we have previously reported that fraudsters can use PII obtained in a data breach to more easily create fraudulent returns that resemble authentic tax returns, making it more difficult for IRS to detect potential fraud.<sup>10</sup>

Even as IRS has adapted its IDT defenses, fraudsters have developed more complex and sophisticated methods to bypass those defenses and commit fraud undetected. IDT refund fraud affects IRS, state revenue offices, tax preparers, tax software companies, and financial institutions. According to industry representatives, as these entities improve security in one area prone to fraud, fraudsters' methods evolve to target a weaker area. For example, in March 2016, IRS alerted payroll and human resource professionals of a phishing e-mail scheme in which fraudsters posed as company executives and requested personal information on employees via e-mail, including W-2s.<sup>11</sup> With this information, fraudsters can imitate the legitimate taxpayer and file fraudulent tax returns seeking refunds. In January 2018, IRS reported that the agency received about 100 reports of W-2 phishing schemes in 2016 and about 900 reports in 2017. IRS also reported that more than 200 employers, affecting hundreds of thousands of employees, were victimized by W-2 phishing schemes in 2017.

---

## IRS Has Broad Efforts Underway to Address IDT and Authentication Challenges

IRS is working to address these challenges, in part, by collaborating with industry—including tax software companies, the tax preparer community, and financial institutions—as well as state partners. In March 2015, the former IRS Commissioner convened a Security Summit with industry and states to improve information sharing and fraud detection and to address common challenges. The Summit led to the creation of seven workgroups to combat IDT refund fraud across multiple platforms. Each workgroup is led by three co-leads—one each from IRS, state departments of revenue or state associations, and industry partners. These workgroups

---

<sup>9</sup>Treasury Inspector General for Tax Administration, *Semiannual Report to Congress, April 1, 2017 – September 30, 2017* (Washington, D.C.: Dec. 1, 2017).

<sup>10</sup>[GAO-16-508](#).

<sup>11</sup>Phishing and spear phishing represent a digital form of social engineering that uses authentic looking e-mails, websites, or instant messages that direct an individual to a website that requests information that fraudsters could use to pose as that individual.

---

collaborate on initiatives to improve IDT refund fraud prevention and detection, including authentication.<sup>12</sup>

In 2015, IRS also established the Identity Assurance Office (IAO) to increase insight into authentication and fraud detection needs agency-wide, including authentication services delivered via four channels: telephone, online, in-person, and correspondence (i.e., postal mail—hereafter referred to as mail—or fax). Among other responsibilities, IAO works with stakeholders across IRS to review the agency’s various authentication programs, including assessing risks of current and planned authentication efforts across the four channels and identifying ways to mitigate these risks. In December 2016, IAO released its *IRS Identity Assurance Strategy and Roadmap (Roadmap)* for developing a modern and secure authentication environment for all taxpayers, regardless of how they interact with IRS.

---

## NIST Established New Requirements for Digital Authentication

Among other things, the National Institute of Standards and Technology (NIST) develops and maintains standards, guidelines, recommendations, and research on the security and privacy of information and information systems. In June 2017, NIST released guidance on digital authentication to help agencies improve the security of their identity-proofing and authentication programs.<sup>13</sup> In its new guidance, NIST breaks down the digital identity environment into three separate components of assurance:

---

<sup>12</sup>In November 2017, we reported on IRS’s efforts to collaborate with these partners to detect and prevent IDT refund fraud. Among other things, we found that the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center pilot partially aligned with leading practices for effective pilot design, but IRS did not have plans to improve its alignment. We recommended that IRS take action to ensure the pilot aligns with leading practices and to expand the pilot’s membership and improve states’ and industry partners’ understanding of its benefits. IRS concurred with both recommendations. See GAO, *Identity Theft: Improved Collaboration Could Increase Success of IRS Initiatives to Prevent Refund Fraud*, [GAO-18-20](#) (Washington, D.C.: Nov. 28, 2017).

<sup>13</sup>National Institute of Standards and Technology, *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017). NIST’s new guidance supersedes its previous guidance, NIST SP-800-63-2, *Electronic Authentication Guideline*. According to OMB guidance, agencies generally have a year to implement changes to comply with updated NIST guidance and can request additional time if needed.

- 
1. **Identity proofing:** establishing that the person is actually who they claim to be;
  2. **Authentication:** establishing that the person attempting to access a service is in control of one or more valid authenticators associated with that person's identity; and
  3. **Federation:** the concept that one set of user credentials can be used to access multiple systems.

The guidance directs agencies to assess the risk for each component of identity assurance, rather than conducting a single risk assessment for the entire process. According to NIST officials, this new approach provides flexibility in choosing identity proofing and authentication solutions; aligns with existing, standards-based market offerings; is modular and cost-effective; and enhances individual privacy.

In addition to NIST's new requirements for authentication, recent technology advances and private-sector innovation are providing new options for identity proofing and authenticating users, including in cases where, for example, IRS interacts with taxpayers once a year. Some examples of these technologies include physical biometrics, such as facial recognition, as well as behavioral biometrics, such as voice patterns, computer keystroke or mouse use patterns, swipe patterns, and gait analysis.<sup>14</sup>

---

<sup>14</sup>Authentication using gait analysis involves automatically identifying or confirming a person's identity based on the way they walk. Gait information can be captured over time using, for example, motion sensors embedded in an individual's smartphone.

---

---

## IRS Incorporates Risk and Other Factors to Guide Authentication Decisions for Taxpayer Interactions

---

### IRS Identifies Interactions that Require Authentication and Estimates Risk to Determine Authentication Approach

According to IRS documents and discussions with officials, the agency considers risks to both the taxpayer and IRS when making decisions about how to approach authentication, which is consistent with federal guidelines.<sup>15</sup> In making these decisions, IRS considers how individuals would be affected by the unauthorized release of sensitive information. IRS also considers the impact on the agency, including the potential for financial loss or harm to IRS programs or services, and loss of public trust.

In 2016, IRS identified over 100 interactions between the agency and taxpayers that require authentication. The interactions range in risk level and IRS categorized them based on the potential for incorrect payment of refunds, disclosure of taxpayer information, and critical impacts on IRS operations.<sup>16</sup> High-risk interactions include when an individual taxpayer establishes an online account with IRS, which provides access to prior year tax information and other PII, or when a taxpayer is asked to confirm his identify before IRS processes what the agency considers to be a potentially fraudulent tax return. Lower-risk interactions include paying a tax bill online. According to IRS, as the risk level of taxpayer interactions increases—for example, interactions that involve sensitive financial information—the authentication process becomes more rigorous. This enhanced security helps reduce the possibility that a fraudster can

---

<sup>15</sup>For example, the Office of Management and Budget directs agencies to conduct electronic authentication (e-authentication) risk assessments for electronic transactions, see OMB, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: December 2003). Further, the E-Government Act of 2002 directs agencies to conduct a privacy impact assessment for any information system that collects, maintains, uses, or disseminates personally identifiable information.

<sup>16</sup>Critical impacts on IRS operations include IRS's inability to process tax returns, issue refunds, and provide services to taxpayers (such as mailing tax transcripts) because of widespread fraud or a data breach.

---

successfully authenticate. Further, if tax professionals want to conduct business with IRS online, such as when working on behalf of a client to file a return or request a prior year's tax transcript, they must establish an account and authenticate their identity.

---

## IRS Can Authenticate Taxpayers through One or More Channels

According to IRS, the agency determines the means by which a taxpayer or tax professional can authenticate his or her identity and what data are required during the authentication process to appropriately minimize risk to the agency. IRS officials told us that the agency works to balance potential risks against its resources and mission to provide all taxpayers access to IRS services and support. IRS performs authentication through the following channels.

**Telephone.** Taxpayers can authenticate via telephone with a customer service representative (CSR) for selected higher-risk interactions with IRS, such as in cases of suspected IDT refund fraud. Telephone authentication can require taxpayers to respond to knowledge-based questions that a fraudster would not likely know. For example, for high-risk interactions, taxpayers must answer additional tax return-related questions. Taxpayers who fail to respond correctly to these questions are then required to authenticate in person at a Taxpayer Assistance Center. For certain lower-risk interactions, taxpayers can authenticate through an automated telephone system.

**In-person.** For some interactions with IRS, taxpayers can authenticate their identity directly with an IRS employee at 1 of IRS's approximately 400 Taxpayer Assistance Centers located throughout the country. Taxpayers may need to present one or more government-issued forms of identification and other documents, such as a utility statement, depending on the level of authentication required for the specific interaction.

**Online.** IRS authenticates taxpayers online for both high-risk and lower-risk interactions. For high-risk interactions such as requesting a tax transcript or looking up an Identity Protection Personal Identification Number (IP PIN), taxpayers must pass a multi-factor authentication process using IRS's Secure Access platform. IRS launched Secure Access in June 2016 following the Get Transcript data breach and, as of April 2018, was using it for 11 applications including authentication for Get Transcript, IP PIN, and the online account. Officials told us they plan to implement Secure Access for other IRS applications in 2018. Taxpayers authenticating through Secure Access establish an account by providing IRS with a valid e-mail address, basic personal information, and



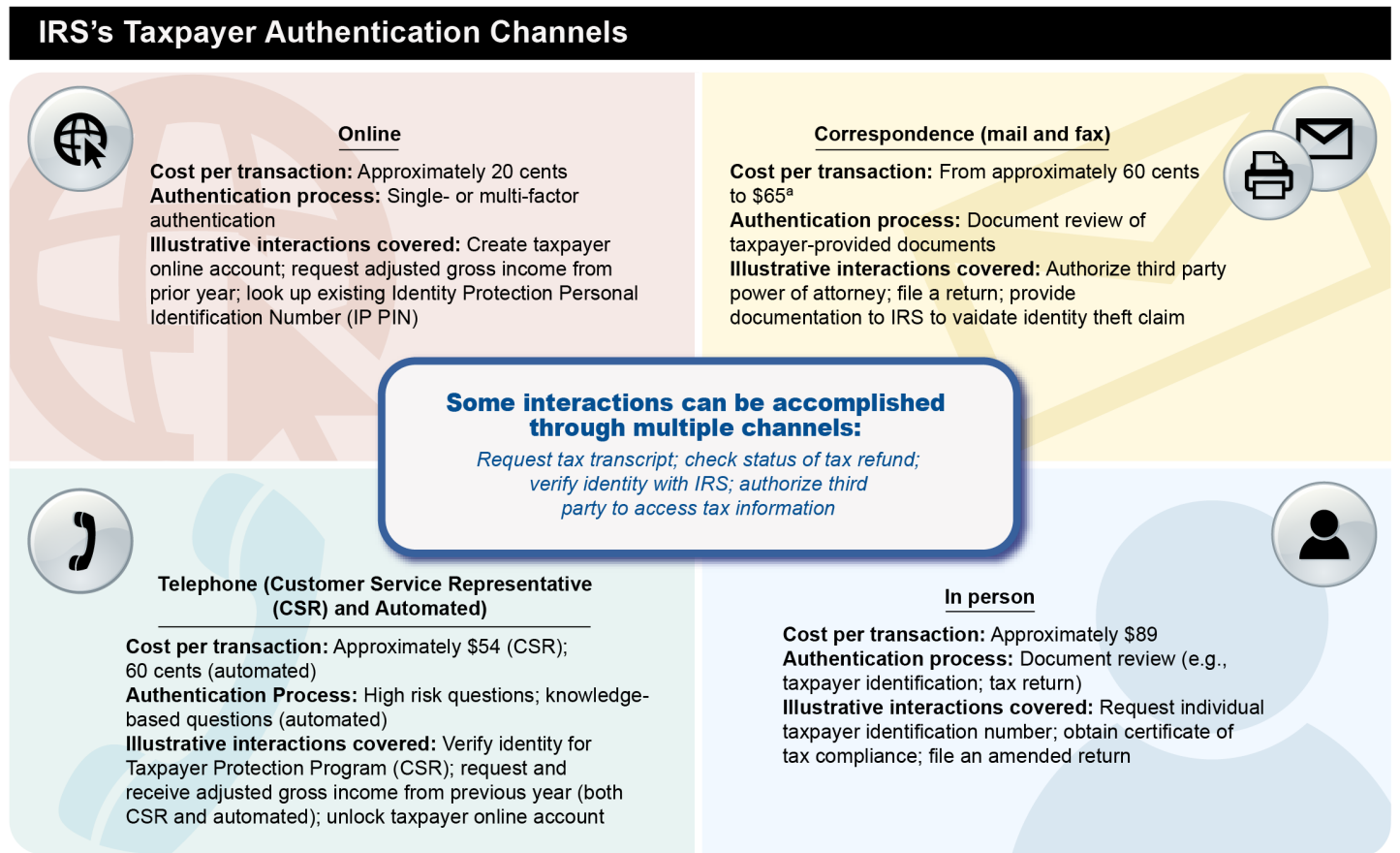
---

personal financial information. Taxpayers then provide IRS a mobile phone number and IRS sends the phone an activation code that the taxpayer enters online. This step validates that the taxpayer possesses the mobile phone. IRS authenticates returning users via a security code. For lower-risk interactions, taxpayers may authenticate online by answering several knowledge-based questions, such as questions about their current return to learn the status of their refund.

**Correspondence.** In some cases, taxpayers can submit documents or request tax information via correspondence, which are then reviewed by IRS and authenticated by matching against information in IRS's systems. This method can require that IRS send the requested documents (such as a tax transcript) only to the taxpayer's address of record, or require the taxpayer to include a photocopy of identification. For example, in some instances, taxpayers who cannot authenticate via telephone and cannot travel to a Taxpayer Assistance Center in person may be able to authenticate by mail.

Each authentication channel requires different IRS resources. These resources include IRS staff and overhead; contracts with vendors that provide identity verification services; and costs inherent to the specific channel, such as mailing costs. Figure 1 summarizes IRS's authentication channels and illustrates a number of the interactions that taxpayers or tax professionals can accomplish through one, or several, channels. It also illustrates the differences in costs per transaction. According to IRS data, in-person authentication at a Taxpayer Assistance Center is the most expensive way to authenticate taxpayers (about \$89 per interaction), followed by telephone (about \$54 per interaction). Online authentication costs the least, at less than \$1 per interaction. According to the National Taxpayer Advocate, while requiring the appropriate level of authentication is necessary to protect IRS against fraudsters, the agency also needs to offer taxpayers a range of options for interacting with IRS.

Figure 1: IRS Authentication Channels and Associated Costs (Based on Fiscal Year 2017 Data)



Source: GAO analysis of Internal Revenue Service (IRS) documents and data. | GAO-18-418

Note: Cost information is rounded to the nearest dollar unless otherwise noted.

<sup>a</sup>According to IRS, selected programs that only require mailing information to taxpayers cost approximately 60 cents for printing and mailing. In contrast, IRS states that inbound correspondence requiring IRS employees to process or verify documents costs about \$65 per transaction.

## IRS's Authentication Programs and Services Are Designed to Reduce Fraud

In this report, we focus on four key IRS programs and services that require authentication:

- **Taxpayer Protection Program (TPP).** Through TPP, IRS reviews tax returns that are flagged by IRS's IDT filters as potentially fraudulent, such as when a return includes characteristics of known fraud schemes. IRS sends a letter notifying taxpayers that they must authenticate their identity before IRS will process the return or issue a

---

refund. According to IRS, in fiscal year 2017, more than 1.9 million taxpayers received such a notification, and IRS authenticated about 1.17 million of them.<sup>17</sup> These taxpayers could verify their identity via telephone, in-person, and correspondence. In August 2016, IRS suspended its TPP online authentication service because of potential system security weaknesses. In mid-March 2018, IRS relaunched the first phase of a more secure TPP online authentication service, which is discussed later in this report.

- **Get Transcript.** This service allows individual taxpayers to request and receive a copy of their prior years' tax information. The transcript contains information from the taxpayer's tax filing history, such as information from Form 1040, *U.S. Individual Income Tax Return*, that can be used, for example, when applying for a mortgage or student loan, or to electronically file (e-file) an upcoming tax return. Taxpayers can request the transcript online or in-person (to be delivered online or via mail); over the telephone (to be delivered via correspondence); or by correspondence (to be delivered via mail). Taxpayers must provide authentication information before IRS will process their request. According to IRS, in fiscal year 2017, IRS delivered about 26.4 million transcripts, with about 59 percent of transcripts delivered online.
- **IP PIN.** IRS assigns each victim of IDT a single-use identification number to be used to file a future electronic or paper tax return. IRS also offers taxpayers in Florida, Georgia, and the District of Columbia the option to request an IP PIN to help prevent IDT in these high tax-related IDT locations. IRS automatically rejects e-filed returns if they do not include the IP PIN and will delay paper returns for extra examination when taxpayers file without the IP PIN. According to IRS, the agency mailed 3.5 million IP PINs to be used during the 2017 filing season.
- **IRS's Online Services.** IRS has developed a number of online services that require taxpayers and tax professionals to authenticate before accessing information online. For example, taxpayers who have established a verified online account can set up an online payment plan. Taxpayers can also check the status of their refund, as well as update their address of record. Taxpayers can also use IRS's mobile application for some of these actions, such as checking the







---

<sup>17</sup>According to IRS officials, cases where taxpayers do not respond to IRS's letter requiring authentication are considered to be fraudulent returns and classified as confirmed fraud.

status of a refund or making a payment to IRS. Similarly, through IRS's e-Services, tax professionals who have been vetted and approved by IRS can manage their e-file accounts, file tax returns on behalf of clients, and view their clients' tax return information.

As noted in figure 2, the volume of taxpayers authenticated for each IRS program or service varies by channel. Further, although TPP costs IRS more than Get Transcript and affects far fewer taxpayers, IRS reported that TPP helped prevent \$5.3 billion in lost tax revenue in calendar year 2016.

**Figure 2: Usage and Costs of Selected IRS Programs and Services That Require Authentication, 2017**

 Program/Service	Number of Users Authenticated by Channel				 Overall Annual Costs
	 Telephone Service	 Online Service	 In-person Service	 Correspondence Service	
Taxpayer Protection Program (TPP)	787,700	N/A <sup>a</sup>	338,400	41,700	at least \$35 million <sup>b</sup>
Get Transcript	6,316,700 <sup>c</sup>	15,600,000	606,700	3,900,000	\$26.1 million
Identity Protection Personal Identification Number (IP PIN)	107,200 <sup>d</sup>	94,000 <sup>e</sup>	N/A	N/A	Data not available
Taxpayer Online Account	N/A	808,000 <sup>f</sup>	N/A	N/A	Data not available

Source: Internal Revenue Service (IRS) documents and data. | GAO-18-418

Notes: Numbers are rounded to the nearest hundred.

N/A = not applicable

<sup>a</sup>Online authentication has not been available for TPP since August 2016.

<sup>b</sup>According to IRS officials, this amount only reflects fiscal year 2017 employee salaries and benefits and does not include other program costs.

<sup>c</sup>Includes customer service representative-supported and automated telephone calls for fiscal year 2017.

<sup>d</sup>Represents IP PINs that were reissued to taxpayers in calendar year 2017.

<sup>e</sup>Represents total IP PINs provided online to eligible taxpayers in filing season 2017.

<sup>f</sup>Taxpayer online account launched on November 16, 2016. This amount includes the number of unique users, irrespective of the number of times each accessed their online account from November 16, 2016, through the end of fiscal year 2017.

---

---

IRS Has Made Progress on Its Authentication Efforts, but Has Not Prioritized Authentication Improvements and Is Not Sufficiently Assessing and Monitoring Risks for All Channels

---

IRS Has Begun to Implement Its Authentication Strategy, but Has Not Articulated Priorities and Resource Needs

IRS has identified high-level strategic campaigns, or efforts to enhance identity assurance, in its *Identity Assurance Strategy and Roadmap (Roadmap)* and has established a business process to support these efforts. However, IRS has not articulated relative priorities for the foundational initiatives supporting its strategic efforts or the resources it will require to complete them. As discussed earlier, IRS's 2016 *Roadmap* is the agency's plan for developing a modern and secure authentication environment for all taxpayers regardless of how they interact with IRS. The *Roadmap* outlines six core authentication objectives, followed by 10 high-level strategic efforts, and 14 foundational initiatives to help IRS address its authentication challenges and identify opportunities for future investment. (See appendix II.) Further, IRS has identified about 90 activities to support its foundational initiatives and the responsible organizations and general duration to complete them.<sup>18</sup> These initiatives include, for example,

- implementing a risk assessment framework that can be applied across all authentication channels and services;

---

<sup>18</sup>These activities vary in scope, ranging from developing manuals and documentation, to broader efforts, such as working with the Security Summit partners to address fraud. The estimated duration to complete each activity also varies, with some taking 6 to 18 months and others taking 3 years or longer.

- 
- developing a framework of identity proofing and authentication requirements for third parties accessing and using IRS data and services; and
  - improving taxpayer assurance by sending automated electronic alerts to taxpayers, such as when they file a return.

To support implementation of these initiatives, IRS established a 12-member executive governance board. Board members are senior executives from business units across IRS, including the Identity Assurance Office (IAO), IT Applications Development, IT Cyber Security, and Wage and Investment. The board helps to monitor progress, risks, and challenges associated with implementing its *Roadmap*, and has generally met monthly since January 2017.

Our prior work on government performance has identified several leading practices for planning at the program or initiative level.<sup>19</sup> Among other things, these practices call for strategic plans to contain the goals and objectives of a program and the human, financial, and information resources required to complete them. Leading practices also call for agencies to develop estimates of benefits and costs to help prioritize new investments.<sup>20</sup> Following these practices can help agencies establish priorities in a complex environment.

IRS has made progress on some of the strategic efforts identified in its *Roadmap*. For example, consistent with its core objectives, IRS has taken steps to enhance fraud detection by improving telephone authentication procedures and expanding its online authentication services. In October 2016, IRS implemented a new process for high-risk telephone authentication, which includes generating questions for the taxpayer using data from internal IRS systems instead of from third-party data or

---

<sup>19</sup>See for example, GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996); *Agencies' Strategic Plan Under GPRA: Key Questions to Facilitate Congressional Review*, [GAO/GGD-10.1.16](#) (Washington, D.C.: May 1997); and *Veterans Health Care: Improvements Needed in Operationalizing Strategic Goals and Objectives*, [GAO-17-50](#) (Washington, D.C.: Oct. 21, 2016).

<sup>20</sup>See Office of Management and Budget, *Guidelines and Discount Rates for Benefit Cost Analysis of Federal Programs*, Circular A-94 (Washington, D.C.: 1992); and GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004).

---

credit reporting agencies.<sup>21</sup> In addition, in March 2018, IRS launched the first phase of its improved online authentication service for TPP, called ID Verify. According to IRS officials, the first phase of the service will be available to taxpayers who did not file the return in question and appear to be victims of IDT refund fraud. The second phase, which IRS plans to implement later in 2018, will expand the service to all taxpayers selected for TPP.

While IRS's *Roadmap* demonstrates the breadth of the agency's strategic vision and core objectives, it does not articulate the resources IRS needs to implement any of its 14 foundational initiatives and their supporting activities. For example, one of IRS's foundational initiatives is to send event-driven notifications to taxpayers, such as when they file a return or request a tax transcript. Such notifications could help IRS detect potentially fraudulent activity at the earliest stage and improve authentication of tax returns. The *Roadmap* identifies seven supporting activities for this foundational initiative. One is to provide taxpayers with greater control over their online accounts. Another supporting activity is to determine methods for sending notifications to taxpayers about activity on their account.<sup>22</sup> However, IRS has not identified the resources required to complete these activities, and the *Roadmap* notes that six of the seven activities will take between 6 months to 3 years to complete. In December 2017, IRS officials stated that they had developed business requirements for the foundational initiative to give taxpayers greater control over their online accounts. However, IRS has not identified funding for the initiative's other supporting activities—such as developing requirements to send push notifications to taxpayers—and implementing them will depend on the availability of future resources.<sup>23</sup>

---

<sup>21</sup>Prior to October 2016, IRS required taxpayers to answer knowledge-based authentication questions drawn from information in public records databases (e.g., credit records) or from the individual's tax records. IRS officials stated that due to the broad availability of PII, and consistent with NIST guidance, they decided to rely only on internal IRS data for authenticating taxpayers for TPP to perform high-risk authentication.

<sup>22</sup>According to IRS, notifications could be sent to the taxpayer via the IRS2Go application, text message, or e-mail. For example, the message could alert the taxpayer that a tax return was filed using the SSN associated with their online account.

<sup>23</sup>In January 2018, IRS officials noted that although this type of alert is not currently available, taxpayers can access their online account to review whether a return has been processed and filed for a current or prior tax year.

---

Further, while IRS has developed a business process that would help the agency prioritize initiatives, the process has not been fully implemented. In 2015, we recommended that IRS estimate and document the costs, benefits, and risks of possible options for taxpayer authentication, in accordance with OMB and NIST guidance.<sup>24</sup> Consistent with our recommendation and its *Roadmap*, IRS developed a process to assess the costs, benefits, and risks of current and potential authentication tools. In May 2017, IRS implemented its business decision model to analyze and improve its online taxpayer authentication services and provided us with results from an analysis for implementing a text-to-voice functionality for IRS's Secure Access online authentication platform. This function would allow taxpayers the option of receiving an automated voice code for authentication on a verified landline (instead of a text message on a mobile phone). As a result of this analysis, IRS approved the proposal to implement this tool. However, in December 2017, IRS officials stated that the text-to-voice tool is not moving forward because of other competing IT improvements and funding constraints. Further, IAO has not yet applied the business decision model to other potential authentication initiatives, such as those identified in its *Roadmap*.

In December 2017, IRS officials stated that each of the strategic efforts and foundational initiatives identified in the *Roadmap* are a high priority, and they are working to address them concurrently while balancing the availability of resources against the greatest threats to the tax environment. We recognize that a strategy is necessarily high-level and that IRS must remain flexible and use necessary resources to respond to unexpected threats. At the same time, clearly identifying resources and prioritizing its initiatives and activities will help clarify the relationships between IRS's authentication efforts and resource needs relative to expected benefits. Further, such efforts may also help IRS establish clearer timelines and better respond to unexpected events.

---

<sup>24</sup>[GAO-15-119](#).



---

---

## IRS Has Not Established a Policy to Assess Risks for Telephone, In-Person, and Correspondence Authentication

While IRS has generally performed regular risk assessments on its online authentication applications, it does not perform comparable assessments to identify, assess, and mitigate risks for its telephone, in-person, and correspondence authentication channels. Federal guidance directs agencies to regularly assess and address the risks of government IT systems.<sup>25</sup> Specifically, OMB requires agencies to conduct annual risk assessments on IT systems performing remote authentication. The assessments should also be conducted when the agency plans to modify its business processes or technology. This includes reviewing new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance outlined in NIST guidance.<sup>26</sup> While federal guidelines broadly require agencies to identify and manage risks and establish specific requirements for programs using online authentication, no corresponding federal guidelines exist for telephone, in-person, and correspondence authentication, although we have previously reported that federal guidance and standards are applicable to IRS's phone authentication.<sup>27</sup>

Similarly, our *Framework for Managing Fraud Risks in Federal Programs* directs agencies to conduct fraud risk assessments at regular intervals and when there are changes to the program operating environment, as assessing fraud risks is an iterative process.<sup>28</sup> Previously, such risk

---

<sup>25</sup>Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, M-04-04 (Washington, D.C.: Dec. 16, 2003); Office of Management and Budget, *Managing Federal Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 28, 2016); and National Institute of Standards and Technology, *Electronic Authentication Guideline, Special Publication 800-63-2* (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).

<sup>26</sup>Per OMB guidance, the assurance level should align with the agency's degree of certainty concerning the consequences of authentication errors and misuse of credentials. Agencies can determine the appropriate level of assurance by conducting an assessment and selecting a technology based on e-authentication technical guidance, among other steps.

<sup>27</sup>Previously, senior IRS officials stated that they disagreed that OMB guidance and NIST digital e-authentication standards are applicable to phone authentication. During the course of our work, officials noted that online authentication occurs entirely remotely, while phone authentication includes some human interaction. However, we have previously reported that the guidance and standards are applicable because TPP uses similar processes to remotely authenticate taxpayers—whether taxpayers respond to questions online or whether the taxpayer answers the questions over the phone with a CSR. See [GAO-16-508](#) for more information.

<sup>28</sup>GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

---

assessments have helped IRS identify security weaknesses and, in some cases, have led the agency to take an authentication service offline. For example, in response to a recommendation we made in May 2016, IRS performed an updated risk assessment on TPP's online authentication service, a key defense against IDT refund fraud.<sup>29</sup> Based on the results of this assessment, IRS disabled its online authentication service until it could appropriately address the security weaknesses that it identified.

Consistent with federal guidance, IRS has identified and analyzed risks associated with services and programs requiring online authentication, including TPP, Get Transcript, and IP PIN, among others. Further, IRS has made recent progress in updating risk assessments and improving security for its online authentication applications. Specifically, between June 2017 and April 2018, IRS reassessed authentication risk levels for some online applications, mitigated risks by moving additional applications behind its Secure Access authentication platform, and identified other compensating controls to appropriately protect its systems.<sup>30</sup> In December 2017, IRS officials stated that they were working to bring remaining authentication applications in line with their most recent risk assessment. They expected to complete this work by the last quarter of fiscal year 2018.

IRS has efforts underway to identify risks for telephone, in-person, and correspondence authentication, but has made limited progress implementing its process for assessing risks for all taxpayer authentication channels. As previously discussed, in 2016, IRS identified over 100 interactions that require taxpayer authentication and categorized these into three high-level risk outcomes. According to IRS's risk assessment process, the next step is for IRS business units to assess the effects of incorrect authentication for each interaction or program, identify gaps in existing processes, and develop options to address the gaps. IRS officials stated that this process involves conducting scenario-based workshops with subject matter experts.

---

<sup>29</sup>[GAO-16-508](#).

<sup>30</sup>Compensating controls, or countermeasures, are used when an agency is unable to implement the recommended control because of, for example, limitations in its IT environment. NIST guidance states that agencies may employ other risk mitigation measures and compensating controls not specified in NIST's guidance.

---

However, as of March 2018, this process has only been applied to TPP and one other IRS business practice.<sup>31</sup> In early 2017, IRS conducted a 2-day, internal, scenario-based workshop to assess risks and impacts and to identify gaps for TPP authentication.<sup>32</sup> Workshop participants identified 45 short-, medium-, and long-term potential enhancements to TPP's authentication processes. However, IRS had not performed similar risk impact assessments for other programs that rely on telephone, in-person, and correspondence authentication—including Get Transcript and IP PIN—and officials do not have a plan or timeline for conducting these assessments. Further, IRS has not developed a plan with time frames to address the deficiencies it identified for TPP. In December 2017, IRS officials stated they are reviewing the 45 TPP enhancements identified by workshop participants, but have no clear plans to implement them because of resource constraints.

IRS has made limited overall progress on this front because it does not have a policy that requires regular assessments and timely mitigation of identified issues for telephone, in-person, and correspondence authentication, as is required for online authentication programs and services. IRS also does not have guidelines for mitigating authentication risks to these channels in a timely manner. In late November 2017, the Director of IAO stated that IAO alone does not have the authority to create and implement a policy that compels other IRS business units to use its risk assessment process or mitigate issues in a timely manner. Officials from other IRS business units stated that they continually assess risks to telephone, in-person and correspondence authentication, even without a policy to do so. However, IRS could not provide evidence of such prior risk assessments or risk mitigation plans. IRS's *Roadmap* states that it will implement a secure authentication platform for taxpayers regardless of how they interact with IRS—online, via telephone, in-person, or correspondence—to help ensure that information is secure and that the agency is interacting with a legitimate taxpayer. Without a policy for conducting risk assessments for these channels and addressing deficiencies in a timely manner, IRS may underestimate known risks and overlook emerging threats to the tax environment. As a result, these

---

<sup>31</sup>In July 2016, IRS conducted an internal workshop to assess risks associated with its change of address business processes and propose mitigation strategies.

<sup>32</sup>These workshops involved subject matter experts across IRS including IAO, IRS's Research, Applied Analytics, and Statistics division (RAAS), and RICS.

---

channels may be more vulnerable to fraudulent activity, including unauthorized attempts to access taxpayer information.

---

## IRS Lacks Internal Controls to Effectively Monitor Telephone, In-Person, and Correspondence Authentication

IRS has established internal controls including procedures and mechanisms to monitor performance of online authentication, but does not have similar controls in place to monitor the performance of telephone, in-person, and correspondence authentication. Federal standards for internal control call for agencies to design their information systems in a way that meets operational needs and allows the agency to respond to risks. Further, agencies are to collect and use quality information to make informed decisions.<sup>33</sup> Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Further, to have an effective internal control system, agencies should also establish procedures to monitor and evaluate the performance of programs and systems as part of the normal course of operations. To this end, monitoring should be performed on an ongoing basis, and any deficiencies the agency has identified should be addressed in a timely manner. Monitoring activities are even more critical in an environment where the risk of fraud is high because such efforts allow an agency to quickly respond to emerging risks to minimize the impact of fraud.<sup>34</sup> Further, IRS's *Strategic Plan* calls for its organizations to use analytics and research to improve program effectiveness and foster a timely, data-driven decision-making environment.

According to IRS documentation and discussions with officials, the Secure Access online authentication platform allows IRS to conduct near real-time monitoring of taxpayer authentication outcomes.<sup>35</sup> Specifically, for each online service using Secure Access, IRS is able to monitor on a daily basis how many taxpayers registered for an account; rates of successful and unsuccessful identity proofing and verification; and suspicious user patterns, such as multiple login attempts. IRS is also able

---

<sup>33</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

<sup>34</sup>[GAO-15-593SP](#).

<sup>35</sup>We did not perform a technical assessment of Secure Access's monitoring functions as part of our work. In February 2018, the Treasury Inspector General for Tax Administration (TIGTA) found that while IRS's online authentication controls had improved, some monitoring tools had not been fully implemented. See TIGTA, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*, 2018-20-007 (Washington, D.C.: Feb. 5, 2018).

---

to monitor system error codes for specific steps in the authentication process, such as when the secure messaging process fails. IRS officials stated that this enhanced performance monitoring of online authentication began in June 2016, and it is helping IRS determine where in the authentication process taxpayers may be having difficulties and potential causes of the problem.

However, IRS does not have comparable procedures and mechanisms to monitor authentication outcomes for telephone, in-person, and correspondence authentication, particularly for TPP, one of IRS's key defenses against IDT refund fraud.<sup>36</sup> Further, since August 2016, taxpayers have been able to authenticate using only these channels. IRS currently uses its Account Management Services (AMS) to capture telephone and in-person authentication outcomes for TPP; however, as discussed below, this is not an effective mechanism for monitoring authentication outcomes.

AMS is IRS's primary application for recording, storing, and retrieving information on all types of taxpayer interactions over time. IRS's customer service representatives (CSR) use AMS to, among other things, record information related to taxpayer authentication performed over the phone or in person for TPP. According to IRS documentation, AMS includes a field where the CSR is to enter the authentication outcome and also an area where the CSR enters notes on the details of the taxpayer interaction. In the context of TPP, IRS officials stated that CSRs use the notes field to record, for example, the reason why the taxpayer failed the authentication process, and other information important for other CSRs to know. IRS also relies on another application to review the status of TPP cases, such as if a case is open or closed.<sup>37</sup>

To better understand how CSRs are implementing procedures to capture TPP authentication outcomes in AMS, we analyzed data in AMS from January through October 2017. The result of our analysis and related discussions with IRS officials indicate three primary internal controls issues. First, IRS does not have a reliable, direct mechanism to collect data on the number of taxpayers who pass and fail telephone, in-person,

---

<sup>36</sup>In some cases, IRS allows taxpayers to fax additional information to support authentication.

<sup>37</sup>IRS officials stated that this database relies on imported data from other IRS systems, including the Electronic Fraud Detection System, the Return Review Program, and the Dependent Database, among other sources.

---

and correspondence authentication. Second, data quality issues make it difficult for IRS to understand why taxpayers may be failing these authentication processes. Third, the IRS organizations responsible for monitoring these channels do not have access to complete AMS data, making it difficult for IRS to identify potential authentication issues and develop solutions to address them.

**No mechanism to collect reliable, direct data on authentication passes and failures.** As previously discussed, when a taxpayer calls IRS or visits a Taxpayer Assistance Center in regard to a TPP letter, the CSR is to enter the result of the authentication (i.e., pass or fail) into AMS with one of nine codes that accurately reflects the authentication outcome. However, AMS does not have a separate, discrete field where the CSR is to enter this information.<sup>38</sup> The field available to capture authentication information is shared with 68 other issue codes, increasing the likelihood that the CSR may select a more generic issue, such as “identity theft” instead of one of the nine codes designated for TPP.<sup>39</sup> Further, one of the TPP outcome codes, called “other issue,” may be too broad for useful analysis. Of the data we reviewed, we found that about one-third of TPP authentication cases were categorized as “other issue,” which provides no information on the authentication outcome.<sup>40</sup> According to IRS’s procedures, this category is to be used in various scenarios, including when IRS does not have enough information to generate questions for authenticating the taxpayer, and in other cases when a taxpayer fails telephone authentication and must go to a Taxpayer Assistance Center. However, by combining all of these issues into one broad category, IRS has limited insight into the size of each particular problem and may be underestimating the number of taxpayers who fail TPP authentication. Further, IRS does not directly capture the results of correspondence-

---

<sup>38</sup>While we did not conduct a similar analysis of CSR-assisted telephone authentications for Get Transcript and IP PIN, we observed that AMS does not contain issue codes to record authentication outcomes for these programs. CSRs can include authentication outcome information for Get Transcript and IP PIN, but only in the notes field.

<sup>39</sup>See appendix I for additional details on the nine codes designated for TPP.

<sup>40</sup>In addition, the number of TPP cases categorized as “other issue” may actually be larger. As discussed later in this section, IRS’s weekly AMS data extract is limited to the first 5,000 records for each issue area or outcome code. During our analysis, we found that records coded as “other issue” were likely subject to this cutoff for 12 of the 42 weeks of data we reviewed.

---

based authentication in AMS and is therefore unable to monitor pass and failure rates for this channel.<sup>41</sup>

**Issues with data quality.** We selected a generalizable random sample of AMS cases identified as TPP authentication failures for January through October 2017 and identified several data quality issues based on our analysis. First, we found that an estimated 19 percent of cases were categorized as an authentication failure, but the content of the CSR notes indicated otherwise.<sup>42</sup> Further, we could not determine a clear match between the TPP authentication outcome and the CSR notes in an additional estimated 18 percent of cases. For example, in these instances, the CSRs' notes provided no information on why the taxpayer failed authentication, or the notes were clearly unrelated to TPP.

Second, we found that CSRs do not consistently enter useful information in the notes explaining why a taxpayer failed authentication, which could provide IRS management with valuable feedback on characteristics of potential fraud or problem areas for legitimate taxpayers. Specifically, our analysis showed that in an estimated 63 percent of cases, CSRs' notes contained information that was useful or somewhat useful for helping IRS understand why a taxpayer failed authentication.<sup>43</sup> In the estimated 37 percent of cases where we determined that the notes were not useful, CSRs generally documented the outcome (i.e., authentication failure) but not the details on why the taxpayer failed. We recognize that a portion of the TPP authentication failures may represent fraudsters trying to authenticate as a legitimate taxpayer. However, given that IRS's fraud detection systems have a history of high false positive rates, these

---

<sup>41</sup>Correspondence is IRS's least common channel for authenticating taxpayers for TPP. As shown in figure 2, IRS reported that it authenticated about 42,000 taxpayers for TPP through correspondence in 2017.

<sup>42</sup>Estimates for this analysis have a margin of error at the 95 percent confidence level of plus or minus 6 percentage points or less. For additional explanation of our methodology, see appendix I.

<sup>43</sup>This analysis included only records where there was a clear match between the TPP authentication outcome and the content of the CSR notes. Our estimates have a margin of error at the 95 percent confidence level of plus or minus 9 percentage points or less.

---

failures may also represent legitimate taxpayers who may be having trouble authenticating.<sup>44</sup>

Further, while the CSR notes could provide IRS potentially valuable information on why taxpayers may be failing authentication, further data analysis may prove difficult. This is because this information is captured in a free-text notes field, rather than in a drop-down list or other standardized way to record data that can then be analyzed. Further, during our analysis of AMS data, we found variation in the way CSRs enter notes, particularly in their use of abbreviations and shorthand on why a taxpayer failed authentication. Such variation makes systematic data analysis difficult.

According to IRS officials and documents we reviewed, there may be several causes for the data quality issues. For example, as noted earlier, CSRs may not be selecting the correct TPP authentication outcome code because there are too many options and procedures may be unclear. IRS officials also noted that when a taxpayer contacts IRS about TPP authentication, they may want to discuss multiple issues. In these cases, the CSR may choose to record information on another issue instead of the authentication outcome.

**Complete AMS data sets are not readily available for analysis.** In addition to the issues described above, the organizations responsible for monitoring TPP telephone and in-person authentication data do not have access to complete AMS data for TPP. IRS officials responsible for managing TPP told us that they do not have direct access to AMS data reports because they are not the system's business owner. Instead, they receive a weekly extract of AMS data from IRS's IT department. However, officials stated that this weekly data extract is limited to approximately the first 5,000 records for each issue area or outcome code, including the codes for TPP.<sup>45</sup> IRS IT officials stated that they limited the file size of the AMS weekly report because it became too large to share internally via e-mail. IT officials stated that the free-text notes entries in AMS were the main cause for large file sizes. However, this procedure of emailing an

---

<sup>44</sup>In June 2017, the National Taxpayer Advocate reported that IRS's fraud detection systems have a history of high false positive rates. Specifically, the National Taxpayer Advocate reported that in calendar year 2016, the false positive rate for TPP identity theft filters was 53 percent, meaning that of all returns flagged as potentially fraudulent, more than half turned out to be legitimate.

<sup>45</sup>Outcome codes include the nine pass and failure codes for TPP.



---

extract of the data, rather than providing direct access to AMS, makes it difficult for IRS to perform comprehensive analyses and ongoing monitoring for TPP using AMS.

To put this into further context, IRS officials reported that in fiscal year 2017, they authenticated about 1.13 million taxpayers for TPP via telephone and at Taxpayer Assistance Centers.<sup>46</sup> However, we found only about 471,600 records with a TPP outcome code in the AMS data IRS provided to us. This represents only about 42 percent of the records we were expecting to see in AMS. IRS officials stated that the discrepancy was likely due to the AMS record limit described above. Yet, in the course of our analysis, we found that only a small number of outcome codes over 42 weeks appeared to be affected by this record limit. (See appendix I for details.) IRS officials could not confirm additional explanations for the discrepancy in the number of records.

IRS's Office of Research, Applied Analytics, and Statistics (RAAS) performs research and quantitative analysis on TPP and has studied authentication performance. For example, in April 2017, RAAS reported results of a newly implemented TPP authentication procedure and found that while the new procedures helped to reduce call times, CSRs were not following the procedures correctly in an estimated 44 percent of the calls. According to IRS officials, RAAS's research efforts provide IRS management with insight into TPP performance and officials have identified areas where TPP can be improved. However, officials face similar data limitations we described above. Further, officials from IRS's RAAS division stated that they must submit a formal data request with IT in order to receive additional data beyond what is included in the AMS weekly extract. While valuable, these research efforts are not a substitute for ongoing monitoring using complete, reliable data, which would allow IRS to identify and address potential problems in a more timely manner.

IRS officials acknowledged that AMS has limitations and stated that they are in the process of planning a new capability in another system to analyze how taxpayers perform on specific questions during the high-risk

---

<sup>46</sup>As previously discussed, IRS has no clear, direct mechanism to capture authentication pass and failure rates in AMS and uses other IT systems to track the status of open and closed cases for TPP. IRS officials stated that the total of 1.13 million authentications it reported for TPP is derived from its TPP database and reflects the number of closed TPP cases. Officials stated that in order for a case to be closed, the taxpayer would have had to successfully authenticate.

---

authentication process.<sup>47</sup> However, this capability will not address the issues in AMS we described above. Further, as of late November 2017, officials were uncertain when this capability would be implemented because of IT funding constraints. Without effective internal control procedures and mechanisms for collecting authentication outcome data, ensuring data quality, and using these data to perform comprehensive analyses and ongoing monitoring of TPP, IRS will continue to have limited insight into its taxpayer authentication operations. As a result, IRS may be challenged in identifying current and emerging threats to the tax system.

---

### IRS Is Working with Security Summit Partners to Improve Taxpayer Authentication

Through the Security Summit, IRS is working with states, software companies, and financial industry partners to identify how best to address IDT and refund fraud. In February 2018, IRS announced that its key indicators for IDT dropped for the second year in a row and the number of taxpayers who reported they were victims of IDT in 2017 fell by about 40 percent, in part because of the Security Summit's ongoing efforts to stop suspected fraudulent returns from entering tax processing systems. IRS has also included key efforts led by the Security Summit in its Roadmap.

The Security Summit's authentication workgroup leads several initiatives aimed at verifying the authenticity of the taxpayer and the tax return at the time of filing. One initiative involves analyzing data elements that are collected during the tax return preparation and filing process. In filing season 2017, the authentication workgroup collected data on 62 elements, 37 of which were new for that year. These elements included, for example, trusted customer requirements and other characteristics of the return. In addition, in 2016 the authentication workgroup worked with software providers to improve authentication procedures to protect taxpayers against their accounts being taken over by criminals. According to IRS officials, these improvements were some of the most visible to taxpayers because they included new password standards to access tax software and required the use of security questions.

Authentication workgroup leaders also described their efforts to collaborate with industry to address authentication challenges. For example, in 2017, IRS, payroll service providers, and tax software providers expanded the *Form W-2, Wage and Tax Statements (W-2)*

---

<sup>47</sup>This capability is to be implemented in an existing IT tool that CSRs use to generate authentication questions and record taxpayer responses.

---

verification code pilot program. The goal of this program is to verify W-2 data submitted by taxpayers on e-filed individual tax returns, using a unique 16-character verification code printed on the form. According to IRS, verification codes appeared on more than 60 million W-2s issued for tax year 2017, compared with about 27.5 million W-2s issued for tax year 2016.

Overall, co-leads from each of the sectors expressed positive views about the level of commitment and cooperation guiding the Security Summit authentication efforts. Officials with whom we spoke stated that they are dedicated to continuing to address authentication issues collaboratively because they all have an interest in improving authentication to reduce tax refund fraud.

---

## IRS Has Improved Its Authentication Methods, but Additional Actions Could Help Enhance Security

---

### IRS Has Taken Preliminary Steps to Adopt NIST's New Guidance, but Does Not Have a Timeline or Detailed Plans for Full Implementation

As described above, in June 2017, NIST released guidance related to online authentication that agencies will need to implement to ensure they are authenticating users in a secure manner.<sup>48</sup> NIST's guidance is designed to (1) describe the risk management process for selecting appropriate digital identity services and (2) help agencies implement authentication programs that provide reasonable risk-based assurances that a returning user is the same user that previously accessed the service. Adherence to the NIST guidance will help IRS provide reasonable risk-based assurance that the person accessing IRS services is who they claim to be. Further, OMB guidance states that federal legacy systems have 12 months to comply with a new NIST publication, while

---

<sup>48</sup>NIST SP-800-63-3. As of March 2018, IRS was following NIST SP-800-63-2 guidance. In March 2018, NIST officials stated that they have posted frequently asked questions and answers about implementing the guidance on NIST's website and plan to develop other tools, use cases, and a forum for stakeholders to discuss best practices and provide feedback.

---

systems under development or undergoing a major transformation need to use the current revision when deployed.<sup>49</sup>

IRS officials told us they have met with NIST officials and plan to update IRS systems and applications to comply with the new security guidelines. IRS officials also noted that the agency has taken preliminary steps to implement the new guidelines. For example, in December 2017, IRS implemented a more secure authentication option through its mobile app, IRS2Go.<sup>50</sup> After taxpayers link their online account with the mobile app, they can use the app to generate a security code to log into their online account. This option is in line with NIST's new guidance and provides taxpayers with an alternative to receiving the security code via a text message. IRS has also taken other preliminary steps to implement the new NIST guidance, including

- forming a task force to guide the implementation of NIST guidance,
- working with the Security Summit to develop an authentication framework that incorporates the new guidance for state and industry partners,
- starting an analysis to identify gaps between IRS's current authentication procedures and the new NIST guidance, and
- updating authentication procedures.

However, IRS has not yet established detailed plans, including timelines, milestone dates, and resource needs, for fully implementing the new guidance. IRS officials cited several reasons for the delay. They said the agency will have to balance maintaining current authentication programs with developing IT infrastructure to support technologies that are compliant with the new guidance. In addition, officials stated that they will need to take a slower, incremental approach to updating authentication programs because of resource constraints. In March 2018, IRS officials provided us a draft, high-level analysis of IRS systems relative to the new NIST guidance, including some action items to address potential gaps.

---

<sup>49</sup>Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 Revised (Washington, D.C.: July 27, 2016).

<sup>50</sup>NIST classifies some types of authentication methods as having additional risk associated with them and has developed additional security requirements for agencies that choose to use them. Agencies can continue to use these methods for authentication, if they also offer users a more secure, less risky way to authenticate.

---

This preliminary analysis is a first step to help IRS identify gaps between IRS's current authentication methods and the new NIST guidance. However, it does not include steps needed to implement the high-level action items, a timeline with milestones, or the resources needed to implement improvements to bring IRS into compliance with the new NIST guidance. IT officials stated that IRS intends to develop its implementation roadmap through 2018 and begin implementing technical solutions in 2019. However, those officials did not identify the technical solutions nor did they have a prioritization plan or documentation of a timeline to fully implement the new NIST guidance.

Implementing the new NIST guidance and updating authentication programs to be protected by the appropriate level of assurance is consistent with federal standards for internal control and IRS's *Roadmap. Standards for Internal Control* notes that agencies should identify, analyze, and respond to risks, as well as assess whether risk response actions sufficiently reduce risk to an acceptable level. Further, one of IRS's initiatives in its *Roadmap* is to strengthen e-authentication and ensure it is in compliance with federal regulations, which includes guidance from NIST.

Developing a plan that includes timelines with specific milestones and resource needs to implement the new NIST guidance is consistent with leading practices for effective planning and management. Specifically, in our prior work on the Government Performance and Results Act, we found that developing and using specific milestones and timelines to guide and gauge progress toward achieving an agency's desired result is a leading practice for effective strategic planning and management.<sup>51</sup> Further, our body of work on IRS has noted that developing project plans with measurable goals, schedules, and resources can help the agency more effectively plan new projects and initiatives.<sup>52</sup>

---

<sup>51</sup>GAO, *Agency Performance Plans: Examples of Practices That Can Improve Usefulness to Decisionmakers*, [GAO/GGD/AIMD-99-69](#) (Washington, D.C.: Feb. 26, 1999) and *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996).

<sup>52</sup>We have applied these principles in our body of work related to IRS. See, for example, GAO, *IRS Return Selection: Improved Planning, Internal Controls, and Data Would Enhance Large Business Division Efforts to Implement New Compliance Approach*, [GAO-17-324](#) (Washington, D.C.: Mar. 28, 2017) and *Large Partnerships: With Growing Number of Partnerships, IRS Needs to Improve Audit Efficiency*, [GAO-14-732](#) (Washington, D.C.: Sept. 18, 2014).

---

According to IRS officials, IRS must balance the needs of its existing authentication efforts against potential new investments. IRS's gap analysis on current authentication procedures relative to the NIST guidance may help IRS prioritize which improvements are most critical. However, without clear plans, timelines, and milestones for performing this work, IRS may not be positioned to address the most vulnerable areas in a timely manner. IRS's timely implementation of NIST's new guidance is critical, as it can help the agency mitigate potential security weaknesses in its existing online authentication programs.

---

### IRS Does Not Have a Comprehensive Process to Evaluate Technologies That Could Help It Improve Authentication

While IRS has made some progress in improving its authentication programs, the agency lacks a comprehensive, repeatable process to identify and evaluate potential new authentication technologies and approaches. IRS's planning documents have noted a commitment to identify and leverage authentication best practices from outside organizations to protect taxpayer data and support IRS business needs. Specifically, IRS's *Roadmap* states that the agency will leverage leading technology and implementation practices from the private and public sectors through a repeatable environmental scan process and, when appropriate, collaborate with partners to address its authentication needs. Similarly, IRS's *Strategic Plan* notes that the agency will invest in innovative, secure technology needed to protect taxpayer data and support the business needs of the agency and its partners.<sup>53</sup>

IRS officials told us the agency continuously researches new identity assurance processes and technologies and has talked with other agencies, industry groups, and vendors to better understand how particular technology solutions could apply to IRS's environment. Further, according to officials, IRS plans to work with an outside organization to analyze third-party identity proofing and authentication services; however, IRS is in the initial phases of this effort. IRS also recently established the Commissioner's Identity Assurance Executive Steering Committee to help oversee IRS's authentication efforts agency-wide. This committee is intended to serve as an advisory body, creating a forum for agency-wide collaboration, as well as providing guidance and direction for identity assurance implementation. IRS provided us documentation that it reviewed some available authentication technologies and their pros and cons in February 2016, and told us that this research helped them

---

<sup>53</sup>Internal Revenue Service, *Strategic Plan: FY2014-2017* (Washington, D.C.: June 2014).

---

develop their *Roadmap*. However, IRS officials could not provide documentation on more recent evaluations of the broader authentication environment, or evidence of a repeatable, comprehensive process to identify and evaluate available authentication technologies and services.

IRS officials stated that one way the agency evaluates potential technologies is through limited pilots or “innovation studies.” For example, from October 2017 to January 2018, IRS conducted a limited pilot to explore the feasibility of having a third-party identity assurance service provider authenticate taxpayers on behalf of IRS.<sup>54</sup> Officials stated that this pilot was possible because it required little upfront investment by IRS. Specifically, IRS received a grant from NIST to implement it, and officials stated that it required minimal integration with IRS’s IT infrastructure. In January 2018, IRS officials stated they were reviewing the results of the pilot, but had not decided on any next steps. Further, IRS officials stated that the agency is considering other pilots, including one to assist with IRS’s telephone authentication and one to enhance security checks during the Individual Taxpayer Identification Number application process.<sup>55</sup> However, while IRS has completed preliminary planning for these pilots, it has not established priorities or timelines because each pilot requires IT support, for example, to ensure the application can be integrated with IRS’s infrastructure and to make any technical changes. Further, in December 2017, IRS officials stated that all innovation studies were on hold until resources become available.

IRS may benefit from considering new ways of approaching its authentication efforts, as other public and private entities face similar challenges of authenticating users. Our discussions with representatives from industry and financial institutions and with government officials indicate that there is no single, ideal taxpayer authentication solution that will solve IRS’s challenges related to IDT refund fraud. Further, representatives from industry and financial institutions and government officials with whom we spoke advocated a layered approach to authentication that relies on multiple strategies and sources of information, while giving taxpayers options for further protecting their information. Based on our discussions with representatives from industry

---

<sup>54</sup>In December 2017, IRS officials stated that the objective of this pilot was to gain a better understanding of the potential benefits and challenges of working with a third-party identity assurance provider.

<sup>55</sup>IRS issues Individual Taxpayer Identification Numbers to foreign nationals and others who have federal tax reporting or filing requirements and do not qualify for SSNs.

---

and state departments of revenue and government officials, some options IRS could consider include the following:

- **Expanding existing IRS services to further protect taxpayers.** As discussed earlier, IRS's online account offers taxpayers several services, including the ability to set up a payment plan and make payments to IRS and view their tax history. In fiscal year 2017, about 808,000 taxpayers created online accounts, and IRS expects this number to grow.<sup>56</sup> IRS's *Roadmap* has identified enhancing taxpayer assurance by expanding authentication, such as generating and sending event-driven notifications to taxpayers to help IRS authenticate returns, which could help IRS quickly validate legitimate returns.

With this option, IRS may be able to further protect taxpayers from IDT refund fraud. For example, IRS could develop additional functionality for the online account that allows the taxpayer to designate a bank account or a preference for a paper check for receiving a tax refund. If a fraudster filed a return with different information, the return would automatically be rejected. In February 2018, IRS officials stated that their strategic vision includes empowering taxpayers to manage their online account; however, when these services offer the ability to change personal or financial information, there is greater potential for fraudsters to exploit them.

- **Federated model.** A federated authentication approach allows an organization to rely on trusted authentication credentials from another entity to log into its systems, potentially without needing to save information from the trusted source. (See figure 3.)<sup>57</sup> One example of a federated authentication model is when people use their Google or Facebook credentials to log into a different website or mobile application. IRS could use a trusted authentication credential from the private or public sector, or another federal agency. The General Services Administration (GSA) has developed a single sign-on authentication platform for federal agencies called Login.gov.<sup>58</sup> In

---

<sup>56</sup>IRS reported that 407,000 taxpayers created new online accounts between October 2017 and February 2018.

<sup>57</sup>A credential is an object or data structure that associates a user's identity with a user's authenticator (e.g., a password).

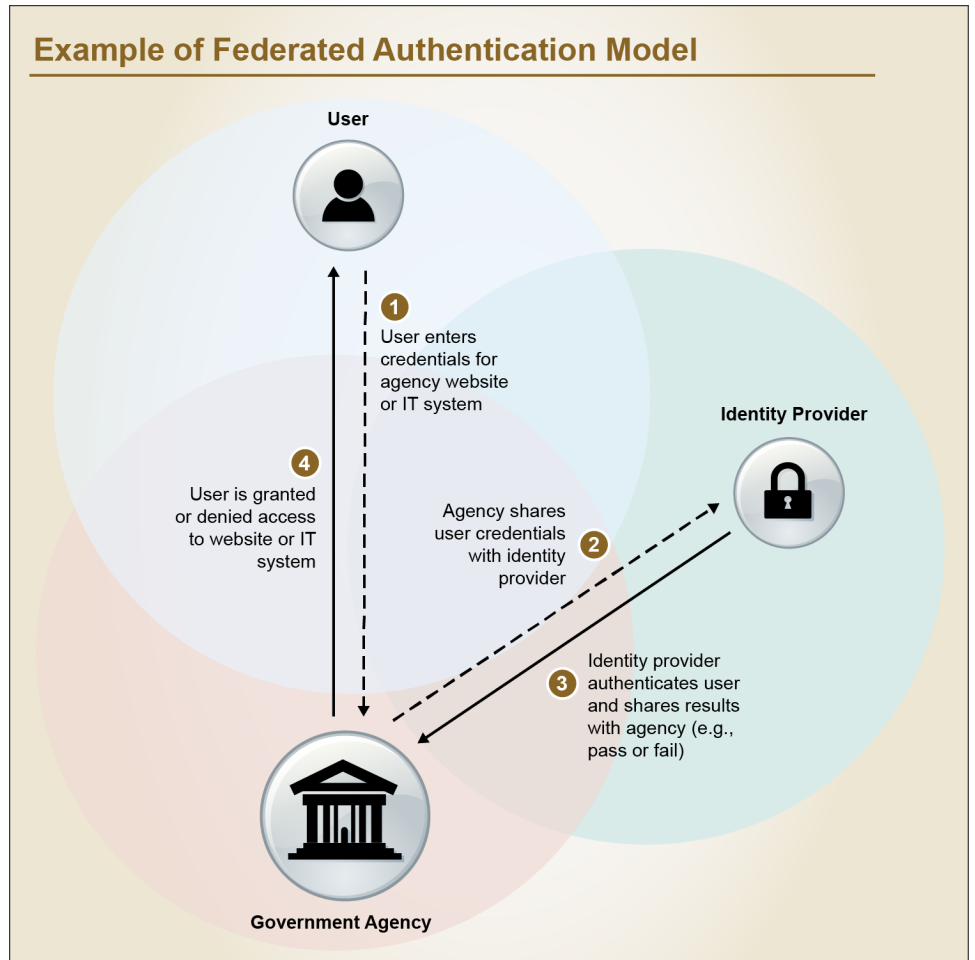
<sup>58</sup>Single sign-on permits a user to use one set of login credentials to access multiple applications.



---

March 2018, GSA officials told us that the Office of Personnel Management and Customers and Border Patrol were using Login.gov and that several other agencies plan to use the authentication platform. According to IRS officials, IRS and Department of the Treasury officials have met with GSA to discuss whether Login.gov could meet IRS's authentication needs. In December 2017, IRS IT officials said they are tracking Login.gov's progress and capabilities and want to ensure that GSA officials understand IRS's requirements. IRS officials said that the agency is interested in being able to federate with different organizations, but does not want to limit federating to one entity, since different taxpayers will want to use different credentials. IRS officials also noted that the agency will need to implement additional IT infrastructure to support a federated model for authentication.

Figure 3: Example of a Federated Model for Authentication



Source: GAO analysis of National Institute of Standards and Technology information. | GAO-18-418

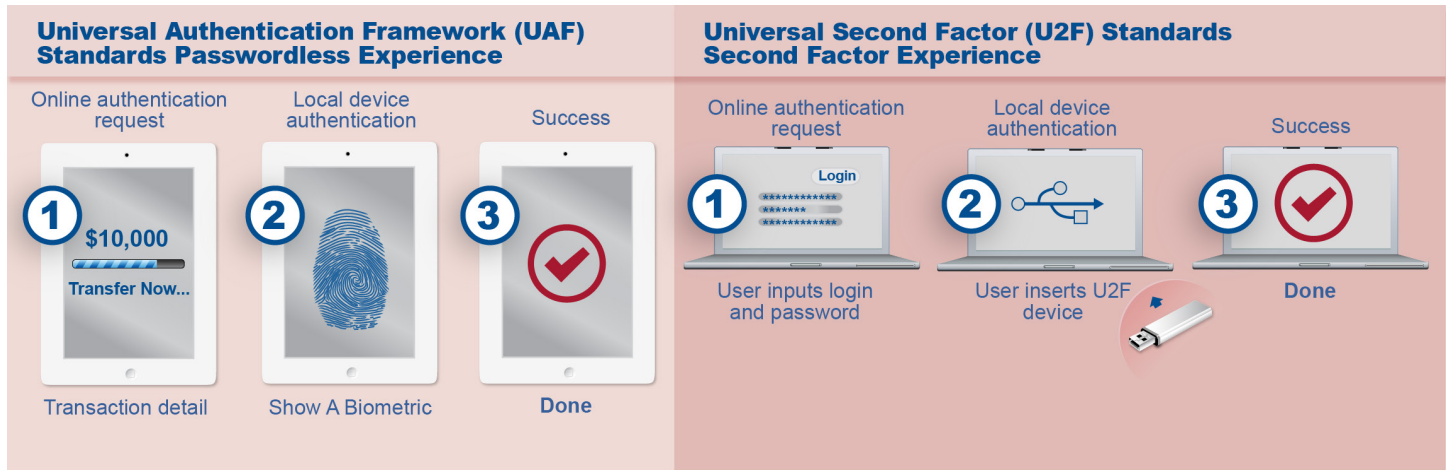
- 
- **Possession-based authentication.** This type of authentication offers users a convenient, added layer of security when used as a second factor for accessing websites or systems that would otherwise rely on a username and password for single-factor authentication.<sup>59</sup> As shown in figure 4, Universal Authentication Framework (UAF) solutions use biometrics, such as an embedded fingerprint, facial recognition, or voice recognition sensor on a computer or smart phone, eliminating the need for a password. Similarly, authentication with a Universal Second Factor (U2F) uses a trusted device or “security key” for authentication in addition to a username and password. According to a representative from the Fast Identity Online (FIDO) Alliance, UAF standards and U2F devices comply with NIST’s new guidance for digital authentication.<sup>60</sup> While IRS is not likely to provide the devices to taxpayers, it could enable its systems to accept these types of standards-based authentication technology for taxpayers who elect to use UAF or U2F devices. For example, taxpayers could use a UAF or U2F device when logging into their IRS online account for additional protection.

---

<sup>59</sup>Both industry and government officials with whom we met noted that data breaches over that past several years have made password-based authentication extremely vulnerable. According to representatives from industry, passwords are a “shared secret,” which the user must give away every time he returns to log into a system. Attackers can exploit this system of revealing a shared secret by either tricking users into thinking that it is safe to reveal their password when it is not, such as through a phishing attempt, or by compromising the servers where the password is stored.

<sup>60</sup>The FIDO Alliance is a nonprofit organization that is working to improve authentication by addressing (1) the lack of interoperability among strong authentication devices, and (2) the need for users to create and remember multiple usernames and passwords. The FIDO Alliance is developing specifications that define open, scalable, and interoperable authentication mechanisms. Companies that have implemented FIDO standards include Bank of America, Google, Microsoft, and Paypal.

Figure 4: Authentication Process Using Universal Authentication Framework and Universal Second Factor



Source: GAO presentation of Fast Identity Online (FIDO) Alliance information. | GAO-18-418

- States' strategies for authentication.** When we met with representatives from five states to discuss how they authenticate taxpayers, representatives from three states volunteered that they use driver's license information to help authenticate taxpayers and tax returns. One state we met with compares driver's license information to other state agency data to help authenticate returns. IRS could investigate making driver's license information, or other government identification, a requirement when filing a federal return, and work with states and other outside organizations to assist with authentication. This information could be a key factor in verifying that the legitimate taxpayer is filing the return. While some industry representatives told us driver's license information is a good credential for identity-proofing, this information can be compromised. For example, fraudsters can use stolen PII to obtain fraudulent driver's licenses.
- Contracting with outside organizations.** Several private-sector organizations offer identity proofing and authentication services. We spoke with officials from the Department of Veterans Affairs (VA) and representatives from the State of Alabama's Department of Revenue, both of which are currently using such services. VA is using a third-party service to identity proof and authenticate veterans accessing services through [www.vets.gov](http://www.vets.gov). For the 2018 filing season, Alabama has contracted with a third-party organization to offer taxpayers a service that sends them an alert when a return is filed using their name, and authenticates the return as legitimate using a selfie. This

---

photo is then digitally compared to their driver's license photo. IRS could evaluate these services to see if any meet their needs.

- **Working with trusted partners.** IRS could partner with organizations it trusts that are accessible to taxpayers and enable the partners to identity-proof and authenticate taxpayers. Trusted partners could include tax preparers, financial institutions, or other federal agencies. In November 2017, IRS officials told us that they had been discussing an in-person identity proofing study with the Social Security Administration (SSA), where SSA would identity proof taxpayers and transmit the authentication data to IRS. However, in June 2018, IRS officials stated that discussions with SSA are ongoing, and they have not made a decision about next steps because SSA is concerned about resources. IRS is also exploring working with the U.S. Postal Service on an information-sharing initiative that could help IRS identify potential IDT.

Throughout the course of our work, IRS officials stated that improving the security of IRS's online authentication applications is a high priority and further noted that IRS must ensure that the highest-risk authentication improvements are completed first. In January 2018, IRS officials stated that the agency's priority is implementing tax reform, which will use IRS's limited IT resources. Further, officials noted that priorities, including resources required to develop project estimates, are determined by IRS's appropriate executive steering committees.

Developing a repeatable, comprehensive process to identify and evaluate different alternatives for taxpayer authentication, such as the ones described above, is consistent with leading practices and can help IRS ensure that it has a sound rationale for its investment decisions.<sup>61</sup> It can also help ensure that IRS has the resources it needs to make authentication improvements in a timely manner. For example, these evaluations may involve developing and documenting a business case for selected initiatives in IRS's *Roadmap*. Such a process could compare options for in-house authentication solutions with solutions available in the private sector based on estimates of cost, schedule, and benefits, as applicable. By identifying options and performing such an evaluation, IRS may find, for example, that an authentication technology available in the

---

<sup>61</sup>See, for example, GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004); and GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).

---

private sector already complies with the new NIST guidelines, offers IRS additional fraud detection capabilities, or is less expensive than developing a similar capability in-house. On the other hand, the process may show that minor improvements to a technology IRS is already using can provide the most secure option in relatively short time, given appropriate resources. This information could be communicated to IRS's executive steering committees, as well as to Congress, to help IRS identify resource needs and ensure it is pursuing the most efficient and effective authentication improvements to protect IRS and taxpayers against evolving threats.

IRS's authentication environment is one component of a broad, complex IT infrastructure, and the agency faces many challenges as it modernizes its tax systems.<sup>62</sup> However, given the availability of PII and the prevalence of cyberattacks, developing a repeatable, comprehensive process to identify and evaluate alternative options for taxpayer authentication and implementing improvements can help IRS ensure it is authenticating taxpayers in the most secure manner. IRS documentation acknowledges that a hybrid authentication approach using in-house solutions, third-party services, and working with trusted partners is the best approach to implementing the new NIST guidance and expanding IRS's authentication coverage. However, without a process to comprehensively identify and evaluate available or emerging authentication technologies and models, IRS may be missing an opportunity to implement the most secure, robust technologies to authenticate and protect taxpayers. Further, including these authentication options and prioritizing them with other initiatives included in IRS's *Roadmap* would help IRS ensure it is working on the highest priority authentication improvements first. It also provides a way for IRS to communicate its strategy and plan for authentication to IRS management and external stakeholders.

---

## Conclusions

Each year, IRS authenticates millions of taxpayers via telephone, online, in-person, or correspondence to verify potentially fraudulent tax returns, provide taxpayers access to a tax transcript, or issue a replacement IP

---

<sup>62</sup>We have reported extensively on IRS's IT modernization efforts. See, for example, GAO, *Information Technology: Management Needs to Address Reporting of IRS Investments' Cost, Schedule, and Scope Information*, [GAO-15-297](#) (Washington, D.C.: Feb. 25, 2015); *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, [GAO-16-468](#) (Washington, D.C.: May 25, 2016); and *Information Technology: Management Attention Is Needed to Successfully Modernize Tax Processing Systems*, [GAO-18-153T](#) (Washington, D.C.: Oct. 4, 2017).

---

PIN. IRS's cost to authenticate taxpayers varies widely, with in-person authentication at a Taxpayer Assistance Center costing about \$89 per interaction and online authentication costing less than \$1 per interaction. The challenge for IRS is to provide taxpayers with options to interact with the agency, while providing IRS with reasonable assurance that it is authenticating the legitimate taxpayer.

In its *Roadmap*, IRS has identified high-level strategic efforts and numerous foundational initiatives to address its most pressing authentication challenges. IRS has made progress in several areas identified in its *Roadmap*. However, identifying the resources the agency will need to complete its foundational initiatives and further prioritizing them would help IRS better understand the relationship between its competing priorities and limited IT resources. Further, while IRS has made progress in identifying risks and establishing internal control activities to monitor online taxpayer authentication, it has not established equally rigorous controls for telephone, in-person, and correspondence authentication. First, IRS does not have a policy for identifying, assessing, and mitigating risks for these authentication channels. Second, IRS does not have effective internal controls for collecting reliable, useful data on telephone, in-person, and correspondence authentication outcomes for TPP and for using these data to monitor authentication operations. Without effective controls for collecting these data and using it for monitoring, IRS may not be positioned to identify potential vulnerabilities in its operations and the necessary improvements.

Given the widespread availability of PII that fraudsters can use to perpetrate tax fraud, it is essential for IRS to strengthen taxpayer authentication to stay ahead of fraudsters' schemes. Completing an analysis of IRS's current authentication procedures relative to new NIST guidance may help IRS identify and prioritize which improvements are most critical. Developing a timeline with milestones and resource needs to implement NIST's new guidance can help guide IRS's implementation and help officials gauge progress and ensure the most critical improvements are made in a timely manner. Further, implementing NIST's new guidance can help IRS ensure its online authentication applications are appropriately protecting IRS information. While improving IRS's current authentication programs would help IRS further protect taxpayer information and identify and prevent fraud, IRS may not need to conduct all of its taxpayer authentication activities in-house nor build IRS-specific authentication solutions: there are many additional tools and partners IRS could consider. Further, developing a repeatable, comprehensive process to identify and evaluate potential authentication

---

technologies and services will help IRS avoid missing opportunities for improving authentication. Further, including and prioritizing these authentication technologies and services in IRS's *Roadmap* could provide useful information to decision makers given IRS's concerns over competing IT priorities and limited resources.

---

## Recommendations for Executive Action

We are making the following 11 recommendations to IRS:

The Commissioner of Internal Revenue should direct the Identity Assurance Office, in collaboration with other IRS business partners, to estimate the resources (i.e., financial and human) required for the foundational initiatives and supporting activities identified in its *Identity Assurance Strategy and Roadmap*. (Recommendation 1)

Based on the estimates developed in Recommendation 1, the Commissioner of Internal Revenue should direct the Identity Assurance Office to prioritize foundational initiatives in its *Identity Assurance Strategy and Roadmap*. (Recommendation 2)

The Commissioner of Internal Revenue should establish a policy for conducting risk assessments for telephone, in-person, and correspondence channels for authentication. This policy should include, for example, the frequency of assessments to be performed and timeframes for addressing deficiencies. (Recommendation 3)

Consistent with the policy developed in Recommendation 3, the Commissioner of Internal Revenue should direct the Identity Assurance Office and IRS business owners to develop a plan for performing risk assessments for telephone, in-person, and correspondence channels for authentication. (Recommendation 4)

The Commissioner of Internal Revenue should establish a mechanism to collect data on outcomes for telephone, in-person, and correspondence authentication, consistent with federal standards for internal control. (Recommendation 5)

The Commissioner of Internal Revenue should revise or establish, as appropriate, procedures to ensure data quality in the Account Management Services (AMS) consistent with federal standards for internal control. (Recommendation 6)



---

The Commissioner of Internal Revenue should ensure that IRS business units have access to complete AMS data to monitor authentication performance and identify potential issues. (Recommendation 7)

The Commissioner of Internal Revenue should direct the Identity Assurance Office and other appropriate business partners to develop a plan—including a timeline, milestone dates, and resources needed—for implementing changes to its online authentication programs consistent with new NIST guidance. (Recommendation 8)

In accordance with the plan developed in Recommendation 8, the Commissioner of Internal Revenue should implement improvements to IRS's systems to fully implement NIST's new guidance. (Recommendation 9)

The Commissioner of Internal Revenue should develop a repeatable, comprehensive process to identify and evaluate alternative options for improving taxpayer authentication, including technologies in use by industry, states, or other trusted partners. (Recommendation 10)

Based on the approach developed in Recommendation 10, the Commissioner of Internal Revenue should include and prioritize these options, as appropriate, in IRS's *Identity Assurance Strategy and Roadmap*. (Recommendation 11)

---

## Agency Comments and Our Evaluation

We provided a draft of this report to the Commissioner of Internal Revenue for review and comment. In its written comments, which are summarized below and reproduced in appendix III, IRS agreed with our 11 recommendations and stated that it is taking action to address them.

IRS agreed with our recommendations to identify resources and prioritize the foundational authentication initiatives identified in its *Roadmap*. IRS noted that the *Roadmap* is a concept document outlining potential strategic initiatives and IRS has not finalized its approach. IRS stated that once it finalizes its authentication approach, it will estimate the resources required for each initiative and prioritize them, consistent with our recommendation. As stated earlier, we recognize that a strategy is a high-level plan and may need to change based on agency needs. Nevertheless, IRS's timely attention to identifying resources and prioritizing its approved authentication initiatives will better position the agency to respond to known and unknown threats to the tax system.

---

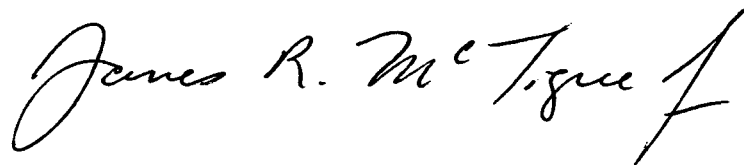
Further, IRS agreed with our recommendations to develop a plan for fully implementing NIST's new authentication guidance and make the necessary improvements to its systems. In its written comments, IRS noted that its ability to complete these efforts will depend on the availability of resources. As noted throughout our report, we recognize the challenge of balancing competing IT priorities and limited resources, but given the importance of implementing authentication improvements consistent with NIST's guidance, we continue to believe it should be a high priority. Additional actions, including addressing our recommendations, will help IRS further mitigate potential security weaknesses in its existing online authentication programs and help prevent potentially hundreds of millions of dollars in fraudulent refunds from being issued.

IRS also agreed with our other seven recommendations, but did not provide additional details on how it plans to address them.

---

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Chairmen and Ranking Members of other Senate and House committees and subcommittees that have appropriation, authorization, and oversight responsibilities for IRS. We will also send copies of the report to the Commissioner of Internal Revenue and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff has any questions about this report, please contact me at (202) 512-9110 or [mctiguej@gao.gov](mailto:mctiguej@gao.gov). Contact points for our offices of Congressional Relations and Public Affairs are on the last page of this report. GAO staff members who made major contributions to this report are listed in appendix IV.



James R. McTigue, Jr.  
Director, Tax Issues  
Strategic Issues

---

*List of Requesters*

The Honorable Orrin Hatch  
Chairman

The Honorable Ron Wyden  
Ranking Member  
Committee on Finance  
United States Senate

The Honorable Kevin Brady  
Chairman

The Honorable Richard Neal  
Ranking Member  
Committee on Ways and Means  
House of Representatives

The Honorable Lynn Jenkins  
Chairman

The Honorable John Lewis  
Ranking Member  
Subcommittee on Oversight  
Committee on Ways and Means  
House of Representatives

The Honorable Vern Buchanan  
Chairman

Subcommittee on Tax Policy  
Committee on Ways and Means  
House of Representatives

The Honorable Peter Roskam  
House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to (1) describe the taxpayer interactions that require authentication, including the general rationale behind the requirements, and the Internal Revenue Service's (IRS) authentication methods; (2) assess what IRS is doing to monitor and improve its authentication methods, both internally and collaboratively through the Security Summit, to secure taxpayer information and reduce identity theft refund fraud; and (3) evaluate what else, if anything, IRS can do to strengthen its authentication methods while improving services to taxpayers.

To describe the interactions that require taxpayer authentication and IRS's methods to do so, we reviewed IRS documents, policies and procedures, IRS data and information on the number of taxpayers authenticated by channel, and interviewed knowledgeable IRS officials. IRS documents and policies we reviewed included IRS's *Authentication Strategy: Current State Touchpoints*, IRS's *Identity Assurance Strategy and Roadmap (Roadmap)*, and Internal Revenue Manuals related to taxpayer authentication. For this report, we focused on the following four IRS programs and services because they require taxpayer authentication, verify a significant number of taxpayer identities each year, and illustrate IRS's different approaches to authentication: the Taxpayer Protection Program (TPP), Get Transcript, Identity Protection Personal Identification Number (IP PIN), and IRS's online services. We reviewed IRS-reported data and information on taxpayer authentication volumes and per transaction costs for these programs for fiscal years 2016 and 2017. To assess the reliability of this data, we examined it for errors and talked with knowledgeable IRS officials. We determined that the data were sufficiently reliable for our purposes. We also interviewed knowledgeable IRS officials on the agency's authentication programs and services to understand different authentication options offered to taxpayers through various channels: in-person, online, telephone, and correspondence.

To assess IRS's efforts to monitor and improve authentication internally and through the Security Summit, we reviewed IRS policies, procedures, authentication risk assessments, and data from IRS systems on authentication performance. We compared IRS's efforts to applicable activities in the *Roadmap*, IRS's *Strategic Plan Fiscal Years 2014-2017 (Strategic Plan)*, *Standards for Internal Control in the Federal Government*, GAO's *Framework for Managing Fraud Risks in Federal Programs*, and relevant National Institute of Standards and Technology (NIST) guidance. We interviewed IRS officials in IRS's Return Integrity and Compliance Services (RICS), Identity Assurance Office (IAO), and Information Technology (IT) knowledgeable about the agency's taxpayer authentication programs. For additional context and informational

purposes, we visited IRS's Andover, Massachusetts call center to observe IRS customer service representatives (CSR) authenticating taxpayers for TPP. We also interviewed IRS, state, and industry co-leads from the Security Summit's Authentication workgroup and Strategic Threat Assessment and Response workgroup to understand IRS's collaborative efforts to improve taxpayer authentication.<sup>1</sup>

To better understand IRS's efforts to authenticate taxpayers via telephone and in person, and how CSRs record data for TPP authentication, we obtained data from IRS's Accounts Management System (AMS) for the weeks January 1, 2017, through October 23, 2017. This was the most recent and complete set of data at the time of our review. We reviewed AMS records coded with any of the nine TPP authentication outcome codes for tax years 2015, 2016, or with "0."<sup>2</sup> We assessed the reliability of the data by: (1) performing electronic testing of key data elements, including checks for missing, out-of-range, or logically inaccurate data; (2) reviewing documents for information about the data and IRS's systems; and (3) interviewing officials knowledgeable about the data to discuss any limitations. During these discussions, IRS officials stated that the AMS data we received may not include all available records in AMS. This is because the IRS office that creates the weekly AMS data report includes only the first 5,000 records for each outcome code. To assess whether this was an issue for our data set, we reviewed record counts for each of the nine TPP outcome codes for the 42 weeks of data IRS provided us. We found 12 out of these 378 instances (3 percent) where the data appeared to be affected by the 5,000 record cutoff. Each of these instances occurred in the "TPP- Other – Sent to TAC" issue code for which we planned no further analysis. Specifically, we did not include this issue code in the generalizable random probability sample described below. As a result, we determined that the data were sufficiently reliable for the purposes of our report.

---

<sup>1</sup>Each Security Summit workgroup is led by three "co-leads"—one each from IRS, state departments of revenue or state associations, and industry partners.

<sup>2</sup>The TPP outcome codes are: (1) TPP – Basic Disclosure Failed; (2) TPP – High Risk Passed; (3) TPP— High Risk Failed; (4) TPP – Out-of-Wallet (OOW) Passed; (5) TPP – OOW Failed/High Risk Failed - Sent to Taxpayer Assistance Center (TAC); (6) TPP – OOW Failed/High Risk Passed; (7) TPP – Other - Sent to TAC; (8) TPP – TAC Failed; (9) TPP – TAC Passed. According to IRS, AMS records coded with a tax year of "0" indicate that either the CSR did not enter a tax year, or it is an entity issue. Entity issues do not correspond to a specific tax year and are related to errors with a taxpayer's name or Social Security number.

To assess the quality and usefulness of the data CSRs enter into AMS for TPP, we selected a random, generalizable sample of records CSRs coded as a TPP authentication failure. We stratified the population into two groups: (1) high-risk authentication failures, and (2) all other authentication failures. From each population, we drew a random sample of 96 records independently, reflecting the population size of each stratum and to be able to detect a 10 percent difference in absolute value between the sample estimate and true population number with a 95 percent confidence level; that is, a 1 out of 20 chance of failure. Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Each sample record was subsequently weighted in the analysis to account statistically for all the cases in the population, including those which were not selected.

Two analysts independently reviewed each sample record to determine (1) whether the TPP authentication outcome code generally aligned with the CSR's notes and (2) the extent to which the CSR notes were useful in understanding why a taxpayer failed authentication.<sup>3</sup> First, the analysts categorized each record in the sample as "aligned" (authentication outcome code and content of CSR notes are clearly aligned); "not aligned" (authentication outcome code and content of CSR notes are clearly not aligned); or "cannot determine" (if the content of the CSR notes was unclear and the analyst could not confidently determine that the record was aligned or not aligned). Next, for each record in the sample, the analysts categorized the content of the notes as one of the following:

- **Useful:** CSR notes provided a clear explanation of why the taxpayer failed authentication (e.g., question failed; taxpayer did not have proper identification; or taxpayer did not have copy of tax return during the call/visit).
- **Somewhat Useful:** CSR notes provided some information on where in the process or why a taxpayer failed, but no clear explanation of the specific reason (e.g., taxpayer passed disclosure, but could not answer high risk questions).

---

<sup>3</sup>For example, if the CSR entered an authentication outcome of "TPP – High Risk Failed," we would expect to see notes describing, for example, that the taxpayer did not have their prior tax year information during the call.

- 
- **Not Useful:** CSR notes were blank, or provided no useful information on where in the process or why a taxpayer failed authentication.
  - **Cannot Determine:** This was selected when the content of the CSR notes was unclear and the analyst could not determine if information was useful.

After the independent review, the analysts discussed their results and resolved any disagreements. Based on these results, we determined how many records in the sample were “aligned,” “not aligned,” or “unable to determine.” Further, we analyzed records categorized as “aligned” to determine how many included CSR notes that were useful, somewhat useful, or not useful.

To evaluate what else, if anything, IRS can do to strengthen its authentication methods while improving services to taxpayers, we interviewed knowledgeable officials from IRS and reviewed documentation to understand IRS’s current authentication methods, future plans for authentication, and challenges IRS faces in taxpayer authentication. We also interviewed knowledgeable officials at the General Services Administration/18F to understand their work on a government-wide authentication platform, Login.gov, and how IRS may be able to use this technology in the future. We also interviewed Department of Veterans Affairs officials to understand how they authenticate veterans applying for benefits at [www.vets.gov](http://www.vets.gov). Further, we met with knowledgeable officials from NIST on their guidelines for online identity-proofing and authentication, which were released in June 2017.<sup>4</sup> To understand current and emerging authentication strategies and technologies, we interviewed representatives from state departments of revenue and from industry. We also interviewed knowledgeable officials from the Office of Management and Budget’s (OMB) U.S. Digital Service to understand their work with IRS in 2016 in launching IRS’s Secure Access online authentication platform and to understand any emerging technologies and standards for authentication. We interviewed a nongeneralizable selection of knowledgeable state and industry representatives based on referrals from NIST officials, and other government and industry representatives knowledgeable on tax issues, including co-chairs from the Security Summit’s Authentication workgroup.

---

<sup>4</sup>National Institute of Standards and Technology, *Electronic Authentication Guideline, Special Publication 800-63-2* (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).

In total we met with representatives from five state departments of revenue, one association representing state tax officials, three financial institution organizations, one financial service industry association, three identity-proofing/authentication organizations, and four tax industry organizations. Finally, we compared IRS's authentication programs and plans for future improvements to its *Roadmap, Standards for Internal Control*, GAO's *Information Technology Investment Management* framework, principles for project planning, GAO's prior work on the Government Performance and Results Act, GAO's *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, and NIST and OMB guidance to determine ways IRS could strengthen its authentication methods, while improving taxpayer service.<sup>5</sup>

We conducted this performance audit from January 2017 to June 2018 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 our findings and conclusions based on our audit objectives.

---

<sup>5</sup>Internal Revenue Service, *Strategic Plan: FY2014-2017* (Washington, D.C.: June 2014); GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004); and GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).; Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 Revised (Washington, D.C.: July 27, 2016); and National Institute of Standards and Technology, *Electronic Authentication Guideline, Special Publication 800-63-2* (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).



# Appendix II: Overview of IRS's Identity Assurance Strategy and Roadmap

**Table 1: Overview of the Internal Revenue Service's (IRS) Identity Assurance Strategy and Roadmap**

Core objectives	High-level strategic efforts	Foundational initiatives
1. Build an omni-channel secure access platform that expands taxpayer coverage and integrates applications/ services across channels	<ul style="list-style-type: none"> <li>Design and apply consistent authentication policies and channel-specific practices to achieve similar levels of assurance for common sets of services / interactions</li> <li>Prioritize technology and processes for e-Authentication to enhance identification, verification, and authorization capabilities as taxpayers continue to shift toward electronically filing.</li> </ul>	<p>Integrate electronic authentication (e-Authentication) registration with additional channels to increase coverage and manage risk</p> <p>Implement and manage an electronic signature program that coordinates policy and oversight while managing risks associated with different IRS documents, forms, and associated third parties</p> <p>Integrate online applications behind e-Authentication, where feasible</p> <p>Strengthen e-Authentication through enhanced identity proofing and expanded coverage, ensuring compliance with federal regulations</p> <p>Conduct virtual in-person identity proofing as part of the e-Authentication registration process, in full compliance with National Institute of Standards and Technology and Office of Management and Budget (OMB) standards</p>
2. Enhance taxpayer assurance by expanding authentication ecosystem	<ul style="list-style-type: none"> <li>Strengthen taxpayer assurance at the point of filing across channels to mitigate the higher level of risk and exposure at this key point of interaction</li> <li>Work with external stakeholders to strengthen authentication capabilities</li> </ul>	<p>Expand W-2 Verification Code Pilot program to enhance assurance at the point of filing</p> <p>Electronically generate and send event-driven notifications to customers opting in to the "At Filing Notification" process to improve taxpayer assurance and IRS authentication of returns</p> <p>Leverage approved external partners as registration agents / trusted referees for enrollment of users in to e-Authentication</p> <p>Develop consistent trust framework of identity proofing and authentication requirements for third-parties access and using IRS data and services</p>
3. Develop fraud detection capabilities to enable proactive prevention and quick detection	<ul style="list-style-type: none"> <li>Predict fraudulent behavior through key risk indicators based on level of risk by channel, expected user patterns based on past behavior, and types of services provided</li> </ul>	<p>Design and leverage fraud indicators through the collection and analysis of user data</p>

**Appendix II: Overview of IRS's Identity Assurance Strategy and Roadmap**

<b>Core objectives</b>	<b>High-level strategic efforts</b>	<b>Foundational initiatives</b>
4. Collect, aggregate, and analyze user data across channels to support authentication, authorization, and access decision making and quick response to incidents	<ul style="list-style-type: none"> <li>Develop and maintain a formal process and ownership roles for capturing data, conducting analysis, and disseminating outputs to appropriate IRS stakeholders</li> </ul>	Build a data gathering and aggregation tool to enable tracking and analysis of customer interactions across touchpoints
5. Operationalize and continuously improve an enterprise response and recovery plan	<ul style="list-style-type: none"> <li>Leverage a response plan that clearly defines incidents and outlines protocols for how they are detected, mitigated, and resolved</li> <li>Build a defined capability and ownership for data detection and retrieval to assess vulnerabilities and determine the scope and magnitude of incidents</li> </ul>	Integrate response plans and protocols to ensure a rapid, coordinated response to fraud incidents and data breaches
6. Implement and provide oversight to a central authentication framework through repeatable processes and governance	<ul style="list-style-type: none"> <li>Ensure that interactions across all channels follow the same authentication-risk standards</li> </ul>	Implement omni-channel risk assessment framework designed to complement the IRS approach to digital authentication assurance and the OMB M-04-04 risk framework
	<ul style="list-style-type: none"> <li>Establish a central authentication policy across the enterprise (i.e., channels and functions)</li> </ul>	Develop a manual documenting all Secure Access enhancements, new functionality, and new services launched behind e-Authentication to ensure consistency in developing, testing, and rolling out new applications

Source: GAO presentation of IRS documents. | GAO-18-418

# Appendix III: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224

JUN 06 2018

Mr. James R. McTigue  
Director, Strategic Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20548

Dear Mr. McTigue:

I have reviewed the draft report entitled *IDENTITY THEFT: IRS Needs to Strengthen Taxpayer Authentication Efforts* (GAO-18-418), and appreciate your acknowledgement of the progress the IRS has made in monitoring and improving our authentication processes. We are continuously challenged with defending the security of the data entrusted to us by U.S. taxpayers in the face of unrelenting attempts by bad actors to defeat our security measures and infiltrate our systems.

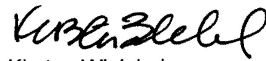
We believe tangible progress has been made in protecting our systems and laying the framework for sound processes that will improve our ability to anticipate and defend against ever-evolving threats. We understand we still have much work to do and appreciate the recognition that a needed next step is defining both the scope of that work and the resources needed to complete it. We agree with the recommendations made in the report and are taking action to address them.

Your report refers to the Identity Assurance Strategy and Roadmap, which is a concept document outlining potential strategic initiatives. Although we continue to assess and determine our direction, we have not finalized and approved our approach for this strategy.

2

Responses to your specific recommendations are enclosed. If you have any questions, please contact Mike Beebe, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (470) 639-3250.

Sincerely,



Kirsten Wielobob  
Deputy Commissioner for  
Services and Enforcement

Enclosure

Enclosure

**Recommendations for Executive Action**

We are making the following 11 recommendations to IRS.

**RECOMMENDATION 1**

The Commissioner of Internal Revenue should direct the Identity Assurance Office, in collaboration with other IRS business partners, to estimate the resources (i.e., financial and human) required for the foundational initiatives and supporting activities identified in its Identity Assurance Strategy and Roadmap.

**COMMENT**

We continue to assess the foundational initiatives recommended in the Identity Assurance Strategy and Roadmap and, once approved, will conduct an estimation of the resources required.

**RECOMMENDATION 2**

Based on the estimates developed in Recommendation 1, the Commissioner of Internal Revenue should direct the Identity Assurance Office to prioritize foundational initiatives in its Identity Assurance Strategy and Roadmap.

**COMMENT**

As noted above, as recommended initiatives are approved, we will prioritize the initiatives inclusive of resource estimates.

**RECOMMENDATION 3**

The Commissioner of Internal Revenue should establish a policy for conducting risk assessments for telephone, in-person, and mail channels for authentication. This policy should include, for example, the frequency of assessments to be performed and timeframes for addressing deficiencies.

**COMMENT**

We agree to assess our policies for conducting risk assessments for telephone, in-person, and mail channels for authentication, including the frequency of assessments to be performed and timeframes for addressing deficiencies.

**RECOMMENDATION 4**

Consistent with the policy developed in Recommendation 3, the Commissioner of Internal Revenue should direct the Identity Assurance Office and IRS business owners to develop a plan for performing risk assessments for telephone, in-person, and mail channels for authentication.

**COMMENT**

We agree with the recommendation that the Commissioner of Internal Revenue will assign and direct the appropriate office to develop a plan for performing risk assessments for telephone, in-person, and mail channels for authentication.

**RECOMMENDATION 5**

The Commissioner of Internal Revenue should establish a mechanism to collect data on outcomes for telephone, in-person, and mail authentication, consistent with federal standards for internal control.

**COMMENT**

We agree with this recommendation and will establish processes for improved data collection for authentication outcomes.

**RECOMMENDATION 6**

The Commissioner of Internal Revenue should revise or establish, as appropriate, procedures to ensure data quality in the Account Management Services (AMS) consistent with federal standards for internal control.

**COMMENT**

We agree with this recommendation and will take the necessary actions to ensure data quality collected within the Account Management Services adheres to federal standards for internal control.

**RECOMMENDATION 7**

The Commissioner of Internal Revenue should ensure that IRS business units have access to complete AMS data to monitor authentication performance and identify potential issues.

**COMMENT**

We agree with this recommendation and will take steps to ensure complete data is available for analysis of authentication performance and identification of other potential issues.

**RECOMMENDATION 8**

The Commissioner of Internal Revenue should direct the Identity Assurance Office and other appropriate business partners to develop a plan, including a timeline, milestone dates, and resources needed, for implementing changes to its online authentication programs consistent with new NIST guidance.

**COMMENT**

We agree with this recommendation and will develop a plan, including a timeline, milestone dates, and resources needed, for implementing changes to our online authentication programs that are consistent with new NIST guidance.

**RECOMMENDATION 9**

In accordance with the plan developed in Recommendation 8, the Commissioner of Internal Revenue should implement improvements to IRS's systems to fully implement NIST's new guidance.

**COMMENT**

We agree with this recommendation. We will implement improvements to our systems to fully implement NIST's new guidance, contingent on resource availability.

**RECOMMENDATION 10**

The Commissioner of Internal Revenue should develop a repeatable, comprehensive process to identify and evaluate alternative options for improving taxpayer authentication, including technologies in use by industry, states, or other trusted partners.

**COMMENT**

We agree with this recommendation. A repeatable, comprehensive process to identify and evaluate alternative options for improving taxpayer authentication, including technologies in use by industry, states, or other trusted partners will be developed.

**RECOMMENDATION 11**

Based on the approach developed in Recommendation 10, the Commissioner of Internal Revenue should include and prioritize these options, as appropriate, in IRS's Identity Assurance Strategy and Roadmap.

**COMMENT**

We agree with this recommendation and will include and prioritize these options, as appropriate, in our Identity Assurance Strategy and Roadmap.

---

# Appendix IV: GAO Contact and Acknowledgments

---

---

**GAO Contact:**

James R. McTigue, Jr. (202)-512-9110 or [mctiguej@gao.gov](mailto:mctiguej@gao.gov)

---

---

**Staff****Acknowledgments:**

In addition to the contact named above, Neil Pinney (Assistant Director), Dawn Bidne, Matthew Bond, Mark Canter, Jehan Chase, Heather A. Collins (Analyst-in-Charge), Michele Fejfar, Robert Gebhart, Steven Flint, Dae Park, and Robert Robinson made significant contributions to this report.



---

# Related GAO Products

---

*Tax Fraud and Noncompliance: IRS Can Strengthen Pre-refund Verification and Explore More Uses.* [GAO-18-224](#). Washington, D.C.: January 30, 2018.

*Identity Theft: Improved Collaboration Could Increase Success of IRS Initiatives to Prevent Refund Fraud.* [GAO-18-20](#). Washington, D.C.: November 28, 2017.

*Financial Audit: IRS's Fiscal Years 2017 and 2016 Financial Statements.* [GAO-18-165](#). Washington, D.C.: November 9, 2017.

*Information Technology: Management Attention Is Needed to Successfully Modernize Tax Processing Systems.* [GAO-18-153T](#). Washington, D.C., October 4, 2017.

*2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits.* [GAO-17-491SP](#). Washington, D.C.: April 26, 2017.

*High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others.* [GAO-17-317](#). Washington, D.C.: February 15, 2017.

*2016 Filing Season: IRS Improved Telephone Service but Needs to Better Assist Identity Theft Victims and Prevent Release of Fraudulent Refunds.* [GAO-17-186](#). Washington, D.C.: January 31, 2017.

*Information Technology: Federal Agencies Need to Address Aging Legacy Systems.* [GAO-16-468](#). Washington, D.C.: May 25, 2016.

*Identity Theft and Tax Fraud: IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program.* [GAO-16-508](#). Washington, D.C.: May 24, 2016.

*Information Security: IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud.* [GAO-16-589T](#). Washington, D.C.: April 12, 2016.

*Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data.* [GAO-16-398](#). Washington, D.C.: March 28, 2016.

---

*Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data.* [GAO-15-337](#). Washington, D.C.: March 19, 2015.

*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.: January 20, 2015.

*Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud.* [GAO-14-633](#). Washington, D.C.: August 20, 2014.

*Internal Revenue Service: 2013 Tax Filing Season Performance to Date and Budget Data.* [GAO-13-541R](#). Washington, D.C.: April 15, 2013.

---

---

## 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 GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

---

## 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 [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail 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:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

---

## Congressional Relations

Orice Williams Brown, Managing Director, [WilliamsO@gao.gov](mailto:WilliamsO@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.