United States Government Accountability Office

Report to the Ranking Member, Committee on Ways and Means, House of Representatives

May 2019

TAXPAYER INFORMATION

IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices

Accessible Version

GAO-19-340

May 2019

TAXPAYER INFORMATION

IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices

GAO Highlights

Highlights of GAO-19-340, a report to the Ranking Member, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

Third-party providers, such as paid tax return preparers and tax preparation software providers, greatly impact IRS's administration of the tax system. If these third parties do not properly secure taxpayers' personal and financial information, taxpayers will be vulnerable to identity theft refund fraud and their sensitive personal information will be at risk of unauthorized disclosure. IRS estimates that it paid out at least $110 million in identity theft tax refund fraud during 2017, and at least $1.6 billion in identity theft tax refund fraud during 2016.

GAO was asked to review IRS's efforts to track, monitor, and deter theft of taxpayer information from third parties. Among other things, this report assesses what is known about the taxpayer information security requirements for the systems used by third-party providers, IRS's processes for monitoring compliance with these requirements, and IRS's requirements for third-party security incident reporting.

GAO analyzed IRS's information security requirements, standards, and guidance for third-party providers and compared them to relevant laws, regulations, and leading practices, such as NIST guidance and *Standards for Internal Control in the Federal Government*. GAO reviewed IRS's monitoring procedures and its requirements and processes for third-party reporting of security incidents, and compared them to Internal Control Standards and GAO's *A Framework for Managing Fraud Risk in Federal Programs*. GAO also interviewed IRS and tax industry group officials.

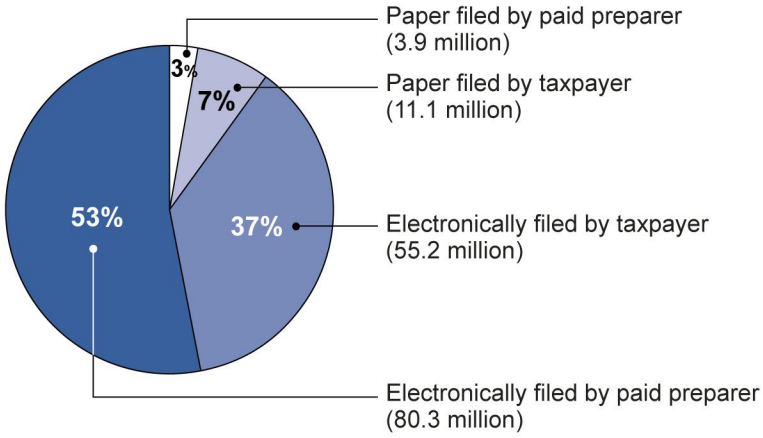
View GAO-19-340. For more information, contact Jessica Lucas-Judy at 202-512-9110 or lucasjudyj@gao.gov

What GAO Found

Federal law and guidance require that the Internal Revenue Service (IRS) protect the confidentiality, integrity, and availability of the sensitive financial and taxpayer information that resides on its systems. However, taxpayer information held by third-party providers—such as paid tax return preparers and tax preparation software providers—generally falls outside of these requirements, according to IRS officials.

In 2018, about 90 percent of individual taxpayers had their tax returns electronically filed by paid preparers or used tax preparation software to prepare and file their own returns.

How Individual Tax Returns Were Filed, Calendar Year 2018



Source: GAO analysis of Internal Revenue Service (IRS) return filing information. I GAO-19-340

IRS seeks to help safeguard electronic tax return filing for various types of third-party providers through requirements under its Authorized e-file Provider program. However, IRS's efforts do not provide assurance that taxpayers' information is being adequately protected.

- Paid Preparers. IRS has not developed minimum information security requirements for the systems used by paid preparers or Authorized e-file Providers. According to IRS's Office of Chief Counsel, IRS does not have the explicit authority to regulate security for these systems. Instead, the Internal Revenue Code gives IRS broad authority to administer and supervise the internal revenue laws. The Department of the Treasury has previously requested additional authority to regulate the competency of all paid preparers; GAO has also suggested that Congress consider granting IRS this authority. Congress has not yet provided such authority. Neither the Department of the Treasury request nor the GAO suggestion included granting IRS authority to regulate the security of paid preparers' systems. Having such authority would enable IRS to establish minimum requirements. Further, having explicit authority to establish security standards for Authorized e-file Providers' systems may help IRS better ensure the protection of taxpayers' information.

What GAO Recommends

GAO suggests that Congress consider providing IRS with explicit authority to establish security requirements for paid preparers' and Authorized e-file Providers' systems.

GAO is also making eight recommendations, including that the Commissioner of Internal Revenue

- Develop a governance structure or other form of centralized leadership to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers.
- Require all tax software providers to adhere to prescribed information security controls.
- Regularly review and update security standards for tax software providers.
- Update IRS's monitoring programs to include basic cybersecurity issues.
- Standardize incident reporting requirements for all types of third-party providers.

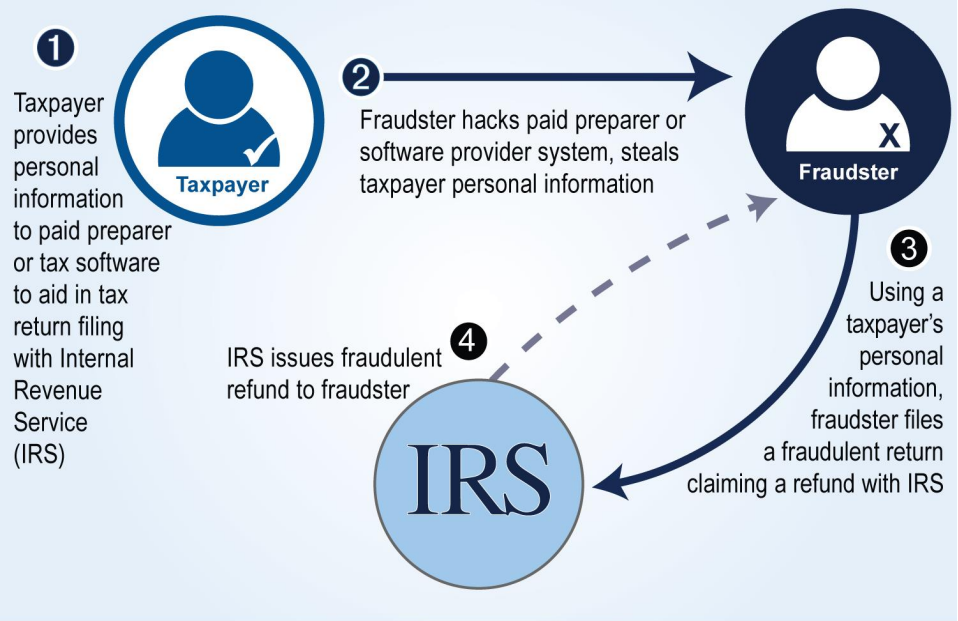
IRS agreed with three recommendations, including the above recommendations to regularly review and update security standards for tax software providers, and standardize incident reporting requirements.

IRS disagreed with five recommendations—including the other three listed above—generally citing the lack of clear and explicit authority it would need to establish security requirements for the information systems of paid preparers and Authorized e-file Providers. GAO believes that IRS can implement these recommendations without additional statutory authority.

- Tax Software Providers. As part of a public-private partnership between IRS and the tax preparation industry, 15 tax software providers voluntarily adhere to a set of about 140 information security controls developed using guidance from the National Institute of Standards and Technology (NIST). However, these controls are not required, and these providers represent only about one-third of all tax software providers. Additionally, IRS established six security, privacy, and business standards for providers of software that allows individuals to prepare their own tax returns (as opposed to software that paid preparers use). However, IRS has not substantially updated these standards since 2010, and they are, at least in part, outdated. For example, IRS cites an outdated encryption standard that NIST recommends not using due to its many known weaknesses.

A key factor contributing to missed opportunities to address third-party cybersecurity is IRS's lack of centralized leadership. Consequently, IRS is less able to ensure that third-party providers adequately protect taxpayers' information, which may result in identity theft refund fraud.

Example of Successful Identity Theft Refund Fraud Attempt



Source: GAO analysis. | GAO-19-340

IRS monitors compliance with its electronic tax return filing program requirements for those paid preparers who electronically file returns; however, IRS's monitoring has a limited focus on cybersecurity issues. For example, the monitoring techniques largely focus on physical security (e.g., locked filing cabinets) rather than verifying that preparers have an information security policy consistent with NIST-recommended controls. Without effective monitoring of cybersecurity controls, IRS has limited assurance that those paid preparers' systems have adequate controls in place to protect clients' data.

IRS recently began collecting information on high-risk security incidents, such as hackers infiltrating third-party provider systems. Reported incidents increased from 2017 to 2018, the only years for which IRS has data. However, IRS does not have a full picture of the scope of incidents because of inconsistent reporting requirements, including no reporting requirements for paid preparers.

Reported High-Risk Security Incidents at Paid Preparers and Tax Software Providers, 2017 and 2018

Category	2017	2018
Number of security incidents	212	336
Number of taxpayer accounts affected	180,557	211,162

GAO analysis of Internal Revenue Service data. | GAO-19-340

Contents

Figures

Abbreviations

CI	Criminal Investigation
e-file	electronic filing
EPSS	Electronic Products and Services Support
ERO	electronic return originator
FISMA	Federal Information Security Modernization Act of 2014
FTC	Federal Trade Commission
ISAC	Identity Theft Tax Refund Fraud - Information Sharing and Analysis Center
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OPR	Office of Professional Responsibility
RICS	Return Integrity and Compliance Services
SB/SE	Small Business / Self-Employed
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
TLS	Transport Layer Security

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 9, 2019

The Honorable Kevin Brady
Ranking Member
Committee on Ways and Means
House of Representatives

Dear Mr. Brady:

Third-party providers, such as paid tax return preparers and tax preparation software providers, have an enormous impact on the Internal Revenue Service's (IRS) administration of the tax system. About 90 percent of individual taxpayers (about 135.5 million in 2018) have their tax returns prepared and filed by paid preparers or use tax software to prepare their own returns. Both paid preparers and tax software providers use taxpayers' personal and financial information to prepare returns, and they may retain that information after returns are filed.

IRS is bound by federal laws to protect taxpayer return information that is filed with, or furnished to, IRS by taxpayers or on their behalf. Generally, those laws do not extend to third-party providers, such as paid preparers and tax software providers, according to IRS officials.[1] If these third parties do not properly secure taxpayers' information, it may be vulnerable to theft or unauthorized use. IRS estimates that at least $11.8 billion in identity theft tax refund fraud was attempted in 2017. According to IRS, it prevented at least $11.7 billion of fraud attempts but paid out at least $0.1 billion to fraudsters.[2]

You asked us to review IRS's efforts to track, monitor, and deter theft of taxpayer information from third-party providers, such as paid preparers

[1]For example, 26 U.S.C. § 6103 and the Federal Information Security Modernization Act of 2014 Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (FISMA 2014). FISMA 2014 largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946-61 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[2]Because of the difficulties in estimating the amount of undetectable fraud, the actual amount could differ from these estimates.

and tax software providers. This report (1) assesses what is known about the taxpayer information security requirements for the systems used by third-party providers, (2) describes IRS's outreach efforts to third-party providers on the requirements, (3) assesses IRS's monitoring processes for ensuring third-party providers' compliance with the requirements, and (4) assesses IRS's requirements for third-party provider security incident reporting and how IRS uses that information.

To assess what is known about the taxpayer information security requirements for the systems used by third-party providers, we reviewed relevant laws and regulations, including the Gramm-Leach-Bliley Act and the Federal Trade Commission's Safeguards Rule, and IRS guidance about information security standards and requirements for third-party providers.[3] To determine whether IRS requirements align with laws and leading practices, we compared the requirements against leading practices, such as the National Institute of Standards and Technology (NIST) Special Publication 800-52 and *Standards for Internal Control in the Federal Government* (Internal Control Standards).[4] We reviewed IRS documents, including organizational charts and associated Internal Revenue Manual (IRM) sections for the offices that have responsibilities for securing taxpayer information.[5] We reviewed Internal Control Standards, which discuss key practices to help an entity adapt to shifting environments, evolving demands, changing risks, and new priorities. We conducted semistructured interviews with 10 industry groups and related organizations that represented a cross section of the tax preparation industry to determine their knowledge about existing information security requirements. We also interviewed IRS officials who were responsible for various aspects of IRS's security requirements for third-party providers.

[3]Gramm-Leach-Bliley Act, Pub. L. No. 106-102, title V, 113 Stat. 1338, 1436-50 (Nov. 12, 1999), *codified at* 15 U.S.C. §§ 6801–6827; Federal Trade Commission Safeguards Rule, 16 C.F.R. pt. 314; Department of the Treasury, Internal Revenue Service Pub. 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* (Rev. 2-2019); and Department of the Treasury, Internal Revenue Service Pub. 3112, *IRS* e-file *Application and Participation,* (Rev. 7-2018).

[4]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014); and National Institute of Standards and Technology, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, Special Publication 800-52, Revision 1 (Gaithersburg, Md.: April 2014).

[5]The IRM is IRS's primary, official compilation of instructions to staff that relate to the administration and operations of the IRS. IRM § 1.11.2 *Internal Revenue Manual (IRM) Process* (Oct. 11, 2018).

To describe the outreach efforts IRS takes for third-party providers, we reviewed IRS outreach documents such as publications, news releases, social media posts, emails, webinars, and online education campaigns. We interviewed IRS officials and conducted semistructured interviews with 10 industry groups and related organizations to identify potential challenges that IRS faces in its outreach.

To assess IRS's monitoring processes for ensuring third-party providers' compliance with information security requirements, we reviewed the agency's monitoring procedures for third-party providers that are authorized to electronically file returns, the related IRM sections, and IRS's monitoring checklist and job aids. We compared these documents to *A Framework for Managing Fraud Risk in Federal Programs* (Fraud Risk Framework).[6] The Fraud Reduction and Data Analytics Act of 2015, and Office of Management and Budget guidance implementing its provisions, affirm that agencies should adhere to the leading practices identified in our Fraud Risk Framework.[7] We reviewed our Fraud Risk Framework principles for combating fraud in a strategic, risk-based manner.[8] We also interviewed the IRS officials responsible for overseeing the monitoring program.

To assess IRS's requirements for third-party provider reporting of security incidents and how IRS uses that information, we reviewed IRS guidance about security incident reporting requirements. We analyzed data on the number and type of security incidents from IRS's Return Integrity and Compliance Services (RICS) Incident Management Database from 2017 and 2018, the only data available following the database's creation in December 2016. We interviewed RICS officials about the quality of these data and determined that IRS's data on the number of security incidents were sufficiently reliable to describe a minimum count of security incidents. Specifically, we asked about the responsibilities of officials collecting and using the data, the procedures in place to capture all reported data, and controls for ensuring the accuracy of the data and resolving any errors, among other things. We also reviewed IRS

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

[7]Pub. L. No. 114-186, § 3, 130 Stat. 546, 546-47 (June 30, 2016); Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (Washington, D.C.: July 15, 2016).

[8]GAO-15-593SP.

documentation and interviewed IRS officials to determine the security incident reporting process through which IRS collects security incident data. We compared that information with leading practices outlined in NIST Special Publication 800-53 and Internal Control Standards.[9] We also used the information from the semistructured interviews with 10 industry groups and related organizations to determine their knowledge about existing security incident reporting requirements. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from November 2017 to May 2019 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.

Background

Federal agencies are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. Cybersecurity—the security of these systems and data—is vital to public confidence. Ensuring the cybersecurity of the nation, including protecting privacy and sensitive data, and IRS's efforts to address tax refund fraud due to identity theft are issues included in our High Risk List.[10]

IRS relies on information system security controls to protect the confidentiality, integrity, and availability of the sensitive financial and taxpayer information that resides on its systems. Federal law and guidance specify requirements for protecting federal information and systems. The *Federal Information Security Modernization Act of 2014* (FISMA) is intended to provide a comprehensive framework for ensuring the effectiveness of information system security controls over information

[9]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

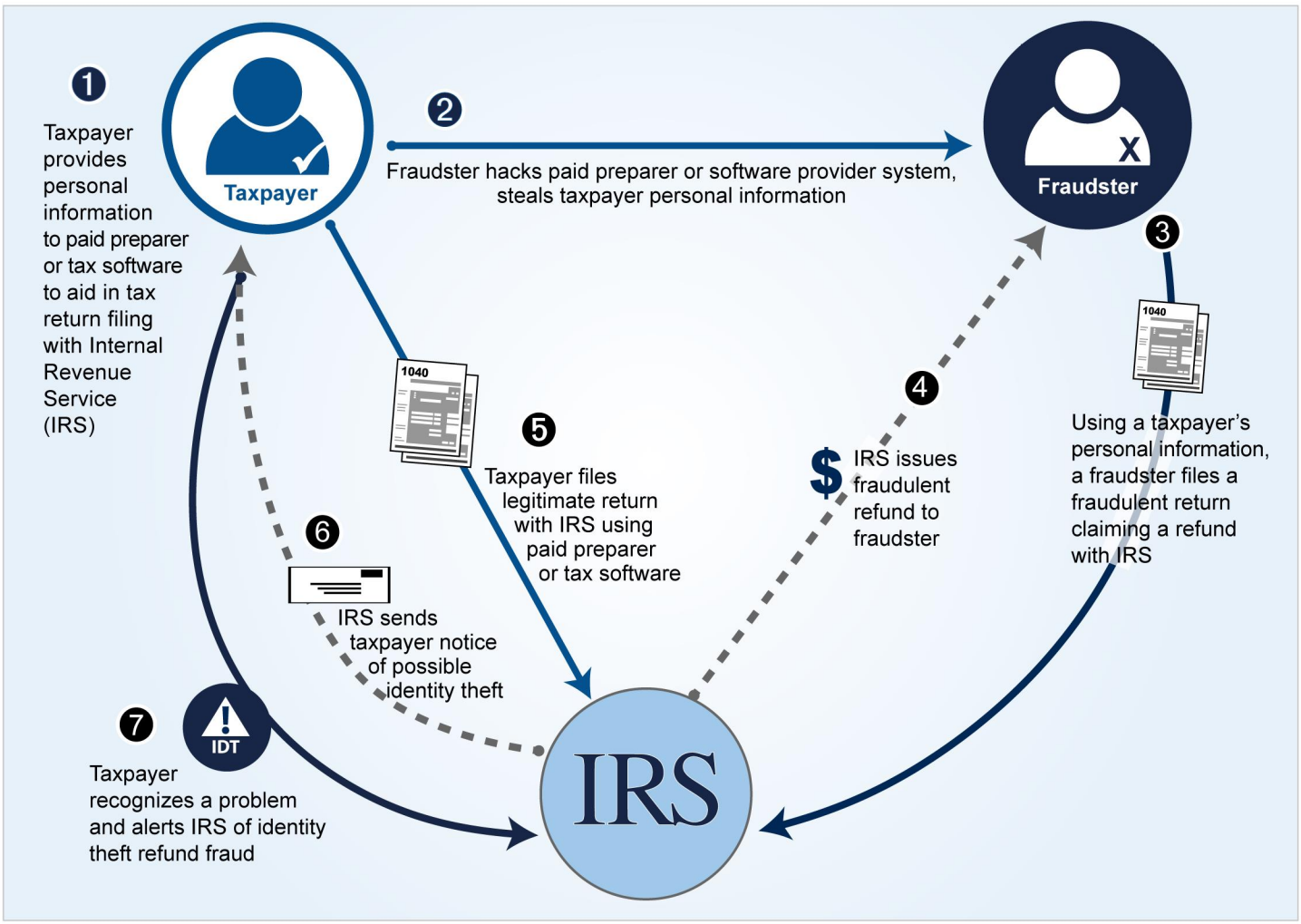
[10]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

resources that support federal operations and assets.[11] To accomplish this, FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and systems that support the operations and assets of the agency, using a risk-based approach. However, taxpayer information held by third-party providers is generally outside of these requirements, according to IRS officials.

Fraudsters may target third parties, such as paid preparers and tax software providers, to steal taxpayer data—defined for our purposes as personally identifiable information and other personal, financial, or federal tax data—which can then be used to commit identity theft refund fraud or other types of financial crimes. Viewed broadly, identity theft tax refund fraud consists of two crimes: (1) stealing or compromising taxpayer data and (2) using stolen (or otherwise compromised) taxpayer data to file a fraudulent tax return and collect a fraudulent refund. Figure 1 presents an example of how this crime can work. In this example, a taxpayer may alert IRS of identity theft refund fraud. Alternatively, IRS can detect identity theft refund fraud through its automated filters that search for specific characteristics, as well as through other reviews of taxpayer returns.

[11]To help implement this legislation, NIST Special Publication 800-53 provides recommended controls to federal agencies and information systems that process, store, or transmit federal information. According to the publication, other organizations are encouraged to consider using these guidelines, as appropriate. See National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

Figure 1: Example of Successful Identity Theft Refund Fraud Attempt



Source: GAO analysis. | GAO-19-340

Third-party providers retain a large amount of electronic tax information, which makes them targets of various types of data theft incidents. Five common types of security incidents are shown in table 1.

Table 1: Common Types of Security Incidents

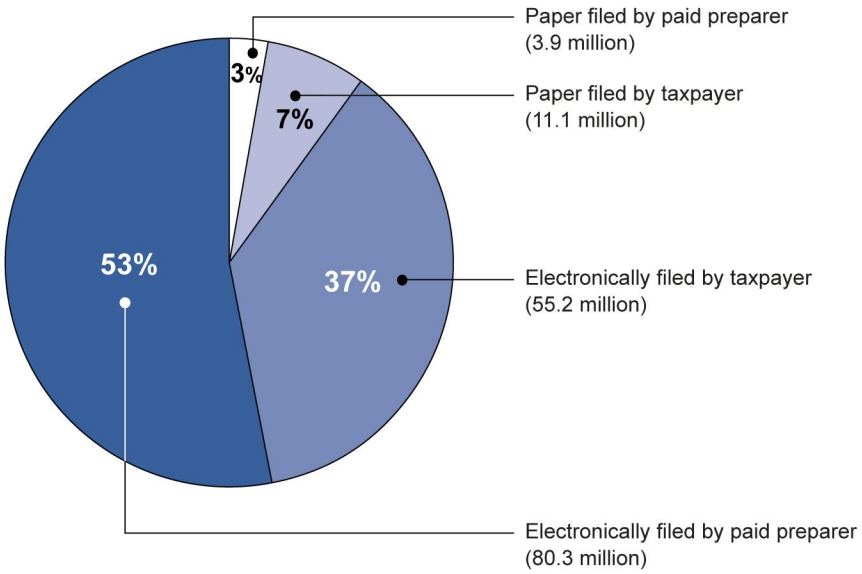
Incident type	Description
Theft	Unauthorized removal of computers, data/records on computer media, or paper files.
Loss/accident	Accidental misplacement or loss of computers, data/records on computer media, or paper files.
Unauthorized access	A person or computer gains access without permission to a network, system, application, data, or other resource.
Unauthorized disclosure/usage	A person knowingly or recklessly makes unauthorized disclosures of tax information or uses the tax information furnished to them in a fraudulent way.
Computer system	A virus, worm, Trojan horse, or other code-based malicious entity infects a host and causes a problem such as disclosure of sensitive data or denial of services.

Source: GAO analysis of Internal Revenue Service information. | GAO-19-340

Note: For more information, see Department of the Treasury, Internal Revenue Service Pub. 4557, *Safeguarding Taxpayer Data, A Guide for Your Business* (Rev. 10-2015).

The number of electronically filed (e-filed) tax returns, and therefore the amount of electronically available data that are vulnerable to security incidents, has been increasing over the past several decades from 4.2 million in 1990 to 135.5 million in 2018. In 2018, approximately 90 percent of the 150.5 million filed individual income tax returns were filed with IRS electronically (see figure 2). Paid preparers prepared more than half of the e-filed returns in 2018.

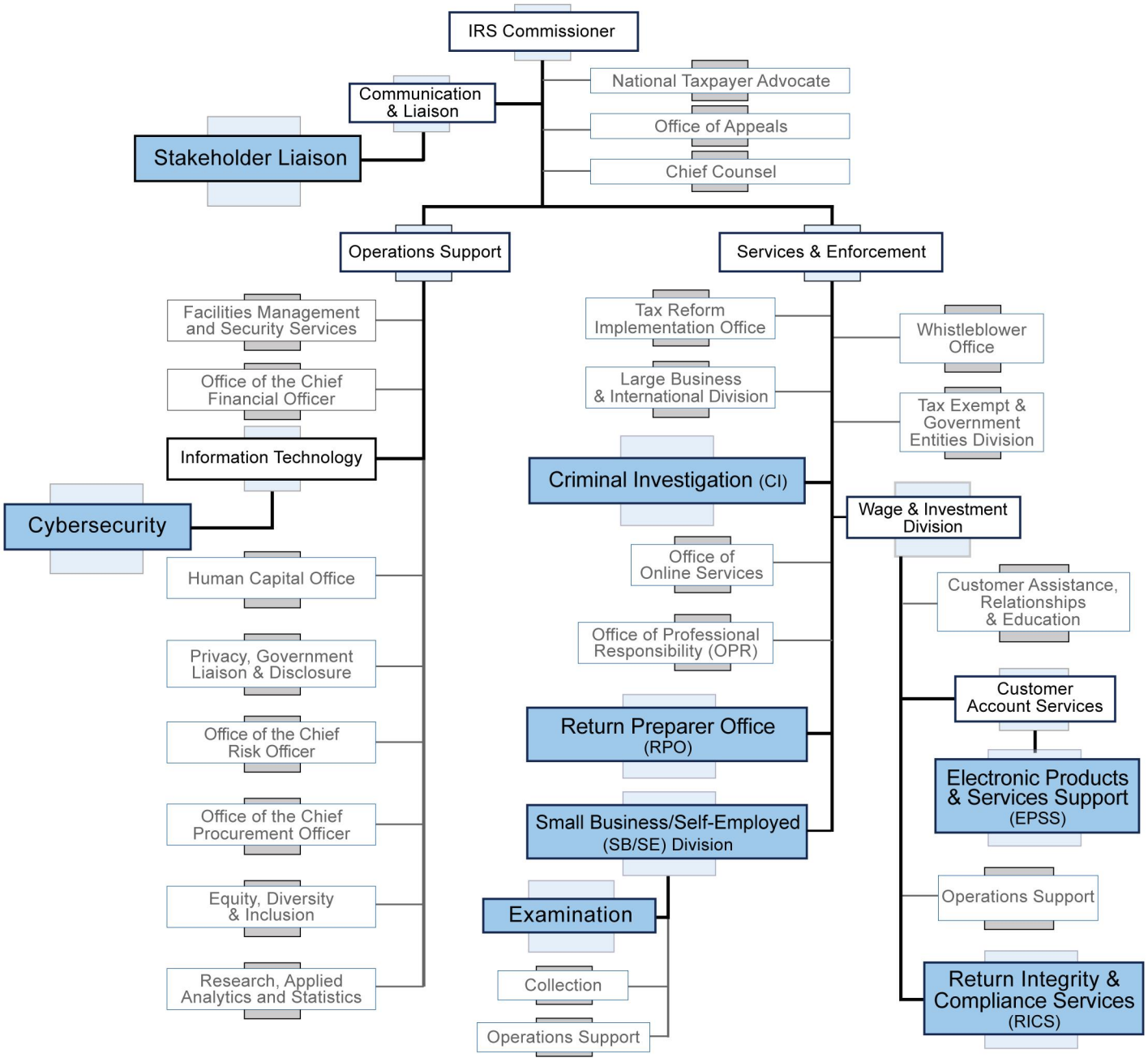
Figure 2: How Individual Income Tax Returns Were Filed, 2018



Source: GAO analysis of Internal Revenue Service (IRS) return filing information. I GAO-19-340

Multiple IRS offices have discrete responsibilities in overseeing how third-party providers secure taxpayer information, as depicted in figure 3.

Figure 3: Internal Revenue Service (IRS) Offices with Some Oversight Functions for How Third-Party Providers Secure Taxpayer Information



Source: GAO analysis of IRS information. | GAO-19-340

Oversight responsibilities are as follows:

- Stakeholder Liaison works with the paid preparer community to educate preparers about information security risks and guide them through the process of resolving security issues when security incidents are reported. This office is also the intake point for security incident information for paid preparers.
- Cybersecurity works to protect taxpayer information and IRS's electronic systems, services, and data from internal and external cybersecurity threats—such as damage to computers, electronic communications systems, or information contained in those systems—by implementing security practices.
- Criminal Investigation (CI) reviews security incident reports to determine whether criminal action has occurred and investigates any potential criminal violations of applicable laws. It also investigates large-scale tax schemes and fraud.
- The Return Preparer Office is responsible for matters relating to the registration and the program compliance of tax return preparers who prepare returns for compensation. The office also engages in outreach and education programs and administers IRS's Annual Filing Season program, a voluntary program to encourage noncredentialed preparers to participate in continuing education courses.
- Small Business/Self-Employed (SB/SE) Examination revenue agents visit e-file providers to ensure they are complying with the Authorized e-file Provider program's requirements.
- Electronic Products and Services Support (EPSS) administers the Authorized e-file Provider program. It is also responsible for updating IRS Publications 1345 and 3112, which outline the requirements of the program. EPSS officials reported that they must coordinate with other business units to update individual references in the publications. EPSS is the intake point for security incident information for online providers and e-Services users, according to officials.
- Return Integrity and Compliance Services (RICS) monitors taxpayer accounts for potential fraud to protect revenue. RICS also manages the security incident data reports that are submitted by tax software providers. RICS is the intake point for security incident information for Security Summit and Identity Theft Tax Refund Fraud - Information Sharing and Analysis Center (ISAC) members, as described below, and actively monitors ISAC alerts from the online platform for new information that may not have been reported elsewhere.

While the Office of Professional Responsibility (OPR) does not have oversight responsibilities over the security of tax information at third parties, it administers the regulations that govern the practice of tax professionals who interact with IRS on behalf of taxpayers, including attorneys, certified public accountants, and enrolled agents, among others.[12] Treasury Department Circular 230, which incorporates the regulations, directed the Commissioner to establish OPR and any other offices within IRS to administer and enforce the regulations. However, Circular 230 does not include a requirement for practitioners concerning the security of taxpayer information.

In recent years, IRS has taken a number of steps to help battle identity theft refund fraud.

- In 2015, IRS formed the Security Summit, a public-private partnership to protect the nation's taxpayers and the tax system from identity theft refund fraud. The summit has representatives from IRS, state tax administrators, and industry partners including the software industry, tax professional associations, and payroll and tax financial product processors.
- IRS launched ISAC in the 2017 filing season. It aims to allow IRS, states, and tax preparation industry partners to quickly share information on identity theft refund fraud. It includes two components: an online platform controlled by IRS to communicate data on suspected fraud, and a collaborative organization governance structure comprising IRS, states, and industry.
- IRS uses a Rapid Response Team in partnership with states and industry members to coordinate responses to identity theft refund fraud incidents. The team aims to respond to significant threats within 24 to 72 hours of their discovery. The Rapid Response Team was deployed for six incidents in 2016, one in 2017, and was not deployed for any incidents in 2018.

[12]31 C.F.R. pt. 10.

IRS's Security Requirements for Third-Party Providers Do Not Provide Assurance That Information Is Being Protected

Different Types of Third Parties Have Varying Responsibilities for Safeguarding Taxpayer Information under IRS's Authorized e-file Provider Program

IRS seeks to help safeguard taxpayers' information and the electronic filing system by prescribing requirements for various types of third-party providers through its Authorized e-file Provider program. These requirements are outlined in Revenue Procedure 2007-40 and Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*. IRS Revenue Procedure 2007-40 states that the security of taxpayer accounts and personal information is a top priority for the agency.[13] Further, the Revenue Procedure states that it is the responsibility of each IRS Authorized e-file Provider to have security systems in place to prevent unauthorized access to taxpayer information by third parties. Some of the requirements included in this program are applicable to all types of Authorized e-file Providers, while others are applicable to one group or another.

Businesses—including sole proprietors—that wish to e-file tax returns on behalf of clients must apply to IRS's Authorized e-file Provider program and choose a provider type, as described in table 2.[14]

[13]IRS Rev. Proc. 2007-40, § 5.03 (June 25, 2007).

[14]IRS outlines the rules for this program in two main publications: Department of the Treasury, Internal Revenue Service Pub. 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* (Rev. 2-2019) and Department of the Treasury, Internal Revenue Service Pub. 3112, *IRS* e-file *Application and Participation,* (Rev. 4-2017). The latter publication includes a full list of all types of Authorized e-file Providers.

Table 2: Selected Authorized e-file Provider Type Descriptions

Provider type	Description
Electronic return originator (ERO)	Originates the electronic submission of tax returns to the Internal Revenue Service (IRS). It may either prepare returns for clients or collect returns from taxpayers who have prepared their own returns. A paid preparer who wants to e-file returns for clients and originate the electronic submission of tax returns to IRS would select this provider option.
Software developer[a]	Writes either origination or transmission software according to IRS specifications, allowing both individuals and paid preparers to file tax returns.
Online provider[b]	Software developer that allows an individual taxpayer to self-prepare returns and file them with IRS via commercially available software, software downloaded from the internet and prepared offline, or through a website.

Source: GAO analysis of IRS information. | GAO-19-340

Note: There are other types of third-party providers beyond those roles discussed in this report. The full list of Authorized e-file Providers is listed in Department of the Treasury, Internal Revenue Service Pub. 3112, *IRS* e-file *Application and Participation* (Rev. 4-2017).

[a]In this report, we refer to software developers as tax software providers.

[b]Online provider is a secondary Authorized e-file Provider role; therefore, they must also be categorized as another provider type, such as software developer. Although an ERO may also use an internet website to obtain information from taxpayers to originate the electronic submission of returns, the ERO is not an online provider.

According to IRS, in 2018 there were more than 325,000 Authorized e-file Providers, some of which were paid preparers. More than 790,000 paid preparers had registered with IRS as of 2018; accordingly, not all paid preparers are Authorized e-file Providers and are therefore not covered by the requirements of the Authorized e-file Provider program. However, a business that has been approved as an electronic return originator (ERO) may employ multiple paid preparers who are not Authorized e-file Providers. Those paid preparers would be allowed to e-file returns under the supervision of their ERO employer. According to IRS Publication 3112, the activities and responsibilities for return preparation and e-filing are distinct and different from each other.

Tax software providers, which IRS refers to as software developers in its Authorized e-file Provider program, develop tax return software that individuals and businesses can use to file their own returns, or that paid preparers can use when filing returns on behalf of clients. Online providers are the subset of tax software providers that allow individual taxpayers to self-prepare returns and file them with IRS. Providers that develop software for paid preparers' use do not fall under the definition of an online provider.

IRS Does Not Fully Incorporate the Federal Trade Commission Safeguards Rule into Its Authorized e-file Provider Program Requirements

IRS has not fully incorporated the Federal Trade Commission (FTC) Safeguards Rule into its requirements for all provider types under the Authorized e-file Provider program. The Gramm-Leach-Bliley Act provided FTC with the authority to require that financial institutions subject to its jurisdiction ensure the security and confidentiality of customer records and nonpublic personal information; protect against any anticipated threats or hazards to the security of such records; and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[15] FTC, in turn, issued a regulation known as the "FTC Safeguards Rule."

The FTC Safeguards Rule applies to financial institutions including third-party providers that help taxpayers file tax returns, such as paid preparers and providers of software that allows individuals to prepare their own tax returns.[16] The FTC Safeguards Rule requires those institutions to develop, implement, and maintain a comprehensive written information security program.[17] The program must contain administrative, technical, and physical safeguards that are appropriate to the provider's size and complexity, the nature and scope of the provider's activities, and the sensitivity of any customer information at issue.[18]

[15]FTC was provided rulemaking authority for developing, implementing, and maintaining reasonable safeguards to protect customer information under the Gramm-Leach-Bliley Act. 15 U.S.C. §§ 6801(b), 6804. The Act includes rules applicable to tax return preparers, some of which are also Authorized e-file Providers, that are designed to ensure the security and privacy of taxpayer information.

[16]Under 16 C.F.R. pt. 314, FTC regulates the protection of customer information at all financial institutions over which FTC has jurisdiction. 16 C.F.R § 313.3(k)(2)(viii) identifies accountants or other tax preparation services as financial institutions for this purpose.

[17]16 C.F.R. § 314.3(a).

[18]On April 4, 2019, FTC issued a proposed amendment to the Safeguards Rule that, if finalized without modification, would include more detailed requirements for the comprehensive information security program required by the rule. Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (proposed April 4, 2019) (to be codified at 16 C.F.R. pt. 314).

IRS addresses the FTC Safeguards Rule through its Revenue Procedure 2007-40. This Revenue Procedure provides the procedures for the Authorized e-file Provider program, and clearly states that violations of the provisions of the Gramm-Leach-Bliley Act and the implementing rules and regulations promulgated by FTC are considered violations of the Revenue Procedure.[19] It also states that violations may subject an Authorized e-file Provider to penalties or sanctions, including suspension or expulsion from the Authorized e-file Provider program.

However, the IRS publications that provide further information on the Authorized e-file Provider program only briefly discuss the FTC Safeguards Rule, and do not provide details on the required elements of an information security program. For example:

- Publication 3112, *IRS* e-file *Application and Participation*, states that providers should become familiar with the Privacy and Security Rules that implement the Gramm-Leach-Bliley Act, and with other important information regarding the safeguarding of personal information available on the FTC website. The publication does not detail each of the required elements of an information security program.
- Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* which was updated in February 2019, notes FTC's role in protecting taxpayer data and generally describes the requirement of implementing and maintaining a comprehensive information security program, including the requirement that administrative, technical, and physical safeguards be appropriate to the business's size, nature and scope of its activities, and the sensitivity of the customer information. The publication does not detail each of the required elements of an information security program.

We identified other IRS publications that are not exclusively related to the Authorized e-file Provider program that discuss the requirements of the FTC Safeguards Rule, as well as other information security measures that serve as leading practices for the broader population of tax professionals. For example, in 2018, IRS updated Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business.* The publication aims to help tax professionals understand basic security steps, recognize signs of data theft, respond to data losses, and understand and comply with the FTC Safeguards Rule. This publication refers to the FTC rule and tax professionals' responsibilities to create and enact security plans, and

[19]IRS Rev. Proc. 2007-40, § 5.03 (June 25, 2007).

provides a checklist from FTC to help third-party providers implement the information security plans. IRS Publication 4600, *Tips for Safeguarding Taxpayer Data*, also discusses elements of the FTC Safeguards Rule. However, while IRS references these documents in Publications 3112 and 1345, Authorized e-file Providers are not obligated to consult or follow these documents.

In addition, most paid preparers do not know about the FTC Safeguards Rule and likely do not have information security plans for their places of business, according to officials from several tax preparation industry groups. Industry group officials also told us that there are misconceptions about who should be responsible for implementing information security. For example, one industry group official said that paid preparers and EROs often think that their tax software providers will provide security services or that their computer firewall or antivirus software will be enough protection.

Modifying the Authorized e-file Provider program requirements to explicitly incorporate the FTC Safeguards Rule's elements of an information security program would be consistent with Internal Control Standards. The standards call for management to consider the external requirements—such as laws, regulations, and standards—and incorporate these requirements into an agency's objectives when setting the standards for the compliance of other entities.

IRS officials told us that they do not believe that federal law provides IRS with any authority to enforce the FTC Safeguards Rule. However, IRS has already stated in Revenue Procedure 2007-40 that compliance with the FTC Safeguards Rule is required for participation in the Authorized e-file Provider program.

Modifying its requirements to explicitly state the elements of an information security program as required under the FTC Safeguards Rule would help IRS ensure that all types of Authorized e-file Providers are aware of, and comply with, the FTC Safeguards Rule, which could help them better protect taxpayers' information.[20] While modifying the

[20]The Electronic Tax Administration Advisory Committee's 2018 annual report to Congress included a recommendation that the FTC Safeguards Rule be extended to all persons providing preparation or filing services for tax returns under the Internal Revenue Code, and that Congress grant IRS the explicit authority to implement and enforce the FTC Safeguards Rule as so extended.

Authorized e-file Provider program may not reach paid preparers who are not part of the Authorized e-file Provider program, it will strengthen the controls for EROs, tax software providers, and online providers.

IRS Lacks Explicit Authority to Require Minimum Security Standards for Paid Preparers' or Authorized e-file Providers' Systems

IRS's Authorized e-file Provider program does not outline a set of minimum information security standards for systems used by paid preparers or Authorized e-file Providers. When we reviewed IRS's publications for Authorized e-file Providers, we found that specific information security standards were outlined for online providers, but there were no specific standards for other types of Authorized e-file Providers or paid preparers.

Officials from tax preparation groups we interviewed and IRS raised issues that relate to paid preparers' system risks. First, the tax preparation industry groups that we spoke with stated that most paid preparers, especially small firms or individual preparers, did not know the steps that they should take to protect taxpayer information on their systems. IRS officials reported that paid preparers often do not know that they experienced a security incident until IRS informs them something is wrong with their filing patterns. Second, according to officials from several tax preparation industry groups, paid preparers often have several misconceptions as to what is required of them in protecting taxpayer data, causing confusion. Industry group officials we interviewed told us that IRS's current publications are not clear about requirements versus leading practices. For example, IRS publication 4557, *Safeguarding Taxpayer Data*, provides paid preparers with some leading practices to protect taxpayer data, but the leading practices are not legal requirements, with the exception of the FTC Safeguards Rule.

An official from the Return Preparer Office explained that imposing any standards for paid preparers, whether related to competency or information security, without explicit authority would leave IRS vulnerable to legal challenges because of a recent court case that found that IRS does not have the authority to regulate the competency of paid

preparers.[21] According to IRS's Office of Chief Counsel, this ruling, combined with the lack of explicit statutory authority, prevents IRS from establishing system standards for paid preparers, because while 31 U.S.C. § 330 authorizes the Secretary of the Treasury to regulate the practice of practitioners before the Department of the Treasury, mere return preparation, including through systems practitioners use to prepare and transmit tax returns, is not considered practice before IRS.[22]

In contrast to paper filing of tax returns, certain security measures need to be taken for e-filing returns to protect the integrity of the e-file system; thus, IRS has implicit authority to regulate e-file providers insofar as their activities relate to electronically filing returns with IRS, according to IRS Office of Chief Counsel officials. These officials also noted that no single provision of the Internal Revenue Code provides IRS explicit authority to regulate the standards for e-file providers. Instead, Internal Revenue Code § 7803 gives the Commissioner of Internal Revenue broad authority to administer and supervise the internal revenue laws, and § 6011 authorizes IRS to require returns and regulate the form of such returns. When taken as a whole, these provisions of the Internal Revenue Code show congressional intent to provide the Secretary of the Treasury with broad authority to administer the method for, and requirements surrounding, the e-filing of federal tax returns, according to IRS officials. Nevertheless, having explicit authority to establish security standards for the systems of Authorized e-file Providers may help IRS better ensure the protection of taxpayers' information and mitigate the risk of legal challenges to IRS's ability to do so.

IRS Office of Chief Counsel officials also noted that for several years the Department of the Treasury has sought additional authority for IRS to regulate all tax return preparers. For example, this request was included in the most recent (fiscal year 2020) Congressional Budget Justification. The justification for this additional authority specifically refers to the competency of tax return preparers, but does not mention security standards for the systems that those preparers use. Similarly, we have previously suggested that Congress consider granting IRS the authority to regulate the competency of paid preparers (that suggestion did not cover

[21]Pursuant to 31 U.S.C. § 330, IRS is authorized to "regulate the practice of representatives of persons before the Department of the Treasury," and the court held that return preparation does not constitute representing persons before IRS. *Loving v. IRS,* 917 F. Supp. 2d 67 (D.D.C. 2013), *aff'd*, 742 F.3d 1013 (D.C. Cir. 2014).

[22]IRS oversees the practice of practitioners before the IRS under Circular 230.

regulating the security of paid preparers' systems).[23] As of April 2019, Congress had not provided such authority.

Without Congress providing IRS with explicit authority to regulate the security requirements for the systems of paid preparers or Authorized e-file Providers, Congress and IRS have limited assurance that the processes used by paid preparers or Authorized e-file Providers are adequately protecting taxpayers' information against electronic data breaches and potential identity theft tax refund fraud. Having such explicit authority would enable IRS to establish minimum security requirements and help ensure improved taxpayer information security by paid preparers and Authorized e-file Providers.

IRS Does Not Have Standardized Security Requirements for All Tax Software Providers

IRS does not have a robust set of information security requirements for all tax software providers in the Authorized e-file Provider program. Instead, IRS has limited security requirements for the subset of tax software providers designated as online providers outlined in IRS Publication 1345, as we discuss in the next section. In Publication 4164, Modernized e-File Guide for Software Developers and Transmitters, IRS also provides some information on "security directive rules of behavior for accessing IRS business systems" while transmitting returns to IRS. However, this document does not provide a specific list of controls to for these providers to follow.

IRS has been working with the Security Summit to implement a subset of the NIST Special Publication 800-53 security and privacy controls for the industry members of the Security Summit, which represents a subset of all tax software providers. The Security Summit partners agreed voluntarily to implement about 140 tax-related controls over a 3-year period and provide self-assessments related to the implementation of those controls. IRS reported in October 2018 that 15 of the 21 Security Summit industry partners had voluntarily certified that they implemented the NIST controls in years 1 and 2 of the rollout schedule. IRS officials

[23]GAO, *Paid Tax Return Preparers: In a Limited Study, Preparers Made Significant Errors,* GAO-14-467T (Washington, D.C.: Apr. 8, 2014). The Joint Committee on Taxation estimated that legislation to regulate paid preparers would increase tax compliance by $135 million in revenue through fiscal year 2025.

reported that they later determined three of the other 21 industry partners are financial institutions that do not handle taxpayer data; thus the standards are not applicable to them. IRS officials told us that they are actively following up with the remaining three providers to determine why they have not completed and submitted the self-assessment, and to what degree they have implemented the subset of NIST security controls.

While this is an important and significant first step, the 15 industry partners in the Security Summit that are voluntarily adhering to the NIST security controls represent about a third of all of the tax software providers that IRS has approved to be a part of the Authorized e-file Provider program. According to IRS, these 15 Security Summit partners transmitted about 132.6 million (98.8 percent) of all of the electronically filed returns in 2018; the other two-thirds of tax software providers in the Authorized e-file Provider program transmitted about 1.6 million (1.2 percent) electronically filed returns. A Security Summit membership criterion states that only those providers that filed more than 50,000 returns with IRS during a filing season can be members, but not all tax software providers meet this threshold.

Internal Control Standards state that managers consider external requirements when defining objectives, such as those set by standard-setting bodies designed to comply with laws, regulations or standards. Management should incorporate those requirements into its objectives and sets those requirements through the established standards of conduct, oversight structure, organizational structure and expectations of competence.

By statue, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. According to Special Publication 800-53, the controls outlined provide a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. While the guidelines in this publication are applicable to all federal information systems, other organizations are encouraged to consider using the guidelines, as appropriate. The applicability of the selected NIST controls is evidenced by the adoption of those controls by the Security Summit partners.

While most returns are filed through tax software providers that are voluntarily adhering to the security controls, these controls are not required and do not apply to all tax software providers. Additionally, IRS officials that are a part of the Security Summit stated that they cannot enforce the subset of NIST controls with the remaining Security Summit partners because the controls were set up in a voluntary program. IRS officials from multiple offices did not have a clear reason as to why this subset of NIST controls has not been incorporated into the requirements for the entire population of tax software providers in the Authorized e-file Provider program, even though some security standards had been incorporated into the Authorized e-file Provider program for a limited set of providers (online providers) as discussed in the next section. In addition, as previously discussed, IRS can prescribe the requirements to which Authorized e-file Providers must adhere when e-filing returns for taxpayers.[24] Incorporating fundamental security controls into its Authorized e-file Provider program would give IRS greater assurance that tax software providers have identified and addressed information security risks consistent with professional standards.

This missed opportunity to update the requirements for tax software providers by adopting the subset of NIST controls is due, in part, to IRS's lack of a centralized leadership over the security of taxpayer information collected by paid preparers and tax software providers. As previously discussed, multiple IRS offices have discrete responsibilities for overseeing the security of taxpayer information while at third parties; however, no one office is responsible for, or has the authority to provide, the strategic vision, oversight, or coordination over all aspects. Further, while IRS offices coordinate to some extent, there is not a formalized governance structure, such as a steering committee, that would help provide this level of leadership, coordination, and collaboration to the agency.

According to Internal Control Standards, an agency's organizational structure provides management's framework for planning, directing, and controlling operations to achieve agency objectives.[25] Management develops an organizational structure with an understanding of overall responsibilities, and assigns these responsibilities to discrete units to enable the organization to operate in an efficient and effective manner

[24]According to IRS officials, 26 U.S.C. §§ 6011, 7803 provide IRS with this authority.

[25]GAO-14-704G.

and reliably report quality information. A sound internal control environment requires that the agency's organizational structure clearly defines key areas of authority and responsibility, and establishes appropriate lines of reporting.

Without setting and requiring the same security standards for all tax software providers, IRS does not have assurance that these providers have an equivalent level of standards in place to adequately protect taxpayer information. Further, in continuing to operate a voluntary security controls program, IRS does not have assurance that those software providers who are currently adhering to the standards will continue to do so in the future. Finally, without centralized leadership in this area, it is unclear how IRS will adapt to changing security threats in the future and ensuring those threats are mitigated.[26]

IRS Has Not Updated the Authorized e-file Provider Program's Information Security Standards for Online Providers Since 2010

Online providers—tax software providers that allow individuals to prepare their own tax returns—have additional requirements for security and privacy that they must follow, as outlined in Publication 1345. IRS established six security, privacy, and business standards for online providers, including requirements for developing information privacy and security policies and reporting security incidents. Compliance with these six standards for online providers became mandatory on January 1, 2010; however, IRS has not substantially updated them since then (see appendix II for the text of the six security, privacy, and business standards). These additional requirements do not apply to paid preparers, EROs, or providers of tax software used by paid preparers.

Without updating standards regularly, the standards can become outdated and lose their ability to protect information from known vulnerabilities as technology changes. For example, IRS's current guidance refers to an outdated encryption standard. Specifically, IRS

[26]The Electronic Tax Administration Advisory Committee reported in 2018 on this same issue. The committee recommended that IRS identify and empower one organization inside the agency with overall responsibility for setting security requirements for tax professionals, and coordinating the implementation of such requirements across IRS stakeholders. See Electronic Tax Administration Advisory Committee, *Annual Report to Congress*, Internal Revenue Service Publication 3415 (June 2018).

requires online providers to use, at minimum, Secure Sockets Layer 3.0 and Transport Layer Security (TLS) 1.0.[27] However, NIST Special Publication 800-52 and industry leading practices recommend the use of TLS 1.1 as the minimum level of encryption due to known weaknesses of using TLS 1.0 to encrypt data in transmission.[28] While the standard allows for use of later encryption versions, it refers to a minimum encryption standard that has known weaknesses. As a result, IRS and taxpayers have limited assurance that their taxpayer data are protected according to NIST guidelines and industry leading practices.

Recommended controls outlined in NIST Special Publication 800-53 and our Fraud Risk Framework call for continuous monitoring and regular fraud risk assessments, respectively, to help determine the effectiveness of controls in a program.[29] Internal Controls Standards also calls for management to periodically review the policies, procedures, and related activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks.[30]

When we asked why the six standards in Publication 1345 had not been updated since 2010, a senior Wage and Investment Division official stated that the publication is subject to an annual review by multiple IRS offices, but no office had identified the need to update the standards as part of these reviews. An Electronic Products and Support Services (EPSS) official told us that the standards were initially developed based on the latest technology at the time. However, according to this official, technology can become obsolete quickly, and adapting standards to keep pace with technological changes can require a lot of resources. Not updating the requirements for online providers again points to a missed opportunity due to IRS's lack of a centralized leadership over the security of taxpayer information at paid preparers and tax software providers. In this case, centralized leadership may have identified the need to update the standards.

[27]Secure Sockets Layers and Transport Layer Security protect sensitive data transmitted over insecure channels, such as by facilitating secure connections between a server and an internet browser.

[28]NIST, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, Special Publication 800-52, Revision 1 (Gaithersburg, Md.: April 2014).

[29]GAO-15-593SP.

[30]GAO-14-704G.

Without periodically reviewing and updating the standards themselves, IRS has limited assurance that the standards have kept pace with technological changes, and therefore, that the online providers are protecting the taxpayer's data.

IRS Uses Various Outreach Techniques to Encourage Third-Party Providers to Protect Taxpayer Information

IRS uses a variety of outreach tools to communicate with third-party providers, such as paid preparers and tax software providers, about information security risks. IRS tries to educate these tax professionals about ways to improve information security practices and the benefits of doing so. For example, IRS informs paid preparers, tax software providers, and others about the importance of reporting security incidents in a timely manner to help ensure that action can be taken quickly to help protect their clients and avoid fraudulent returns being filed. Similarly, Stakeholder Liaison advises paid preparers about the steps to take to ensure that their systems are no longer vulnerable to compromise, according to Stakeholder Liaison officials.

Below are examples of IRS's recent communication efforts.

- IRS and the Security Summit collaborated on tax professional outreach campaigns. For example, in 2018, they launched the Tax Security 101 campaign, which provided tax professionals with basic information on how to protect taxpayer data.
- Each year, IRS sponsors nationwide tax forums largely targeted toward paid preparers such as enrolled agents, certified public accountants, and noncredentialed preparers.[31] The 2018 forum included five seminars focused on securing taxpayer information, such as "Data Privacy and Cybersecurity for Tax Professionals" and "Data Compromises—It's Not a Matter of 'If' but 'When.'"

[31]Enrolled agents licensed by IRS and certified public accountants have unlimited representation rights before IRS, and may represent their clients on any matters including audits, payment or collection issues, and appeals. Preparers who have enrolled and completed the Annual Filing Season Program are entitled to represent taxpayers before IRS in examination of tax returns that they prepared and signed. Preparers with an active Preparer Tax Identification Number, but no professional credentials and do not participate in the Annual Filing Season Program, are authorized to prepare tax returns but have no authority to represent clients before IRS.

- IRS hosts webinars throughout the year to inform tax professionals and taxpayers about various topics, including information security.[32] For instance, in October 2018, IRS hosted a webinar called “Protect Your Clients, Protect Yourself: Tax Security 101.” The webinar covered common security threats, signs of data theft, ways to report taxpayer data theft to IRS, and tax preparers’ obligations to create a written information security plan consistent with the FTC Safeguards Rule.
- Stakeholder Liaison has participated in over 1,000 virtual and in-person events since June 2015 where data security was a primary topic or featured message, according to Stakeholder Liaison officials. Further, the officials reported that there were over 165,000 attendees at these events.
- IRS uses social media outlets such as YouTube and Twitter to provide information to tax professionals. For example, in July and October 2017, IRS released two YouTube videos about information security for tax professionals titled “Why Tax Professionals Need a Security Plan” and “What to Do After a Tax Professional Data Compromise.” Similarly, IRS’s tax professional Twitter account, @IRStaxpros, releases information about information security (see figure 4).

Figure 4: Examples of IRS Tweets to Tax Professionals

Source: Internal Revenue Service (IRS) social media. I GAO-19-340

[32]Internal Revenue Service, *Webinars for Tax Practitioners*, accessed October 22, 2018, https://www.irs.gov/businesses/small-businesses-self-employed/webinars-for-tax-practitioners.

Though IRS has various ways to disseminate information to tax professionals, it faces a challenge reaching paid preparers who are not affiliated with larger industry groups or who do not visit the IRS.gov website, according to both IRS officials and industry group officials. According to Return Preparer Office officials, many paid preparers are not linked to standard tax communication channels, such as direct communications from IRS through news releases or email alerts. IRS and industry group officials told us one barrier to reaching these paid preparers is preparers' belief that their businesses are too small to be a target for fraudsters. IRS officials recognize the challenges and said that they continue to address them by speaking with tax professionals about how to increase paid preparers' awareness of information security risks, such as by making materials easy for preparers to read.

IRS's Authorized e-file Provider Monitoring Largely Focuses on Physical Security Controls and Is Inconsistent among Provider Types

IRS Monitoring Efforts for EROs Have Limited Focus on Cybersecurity

IRS's monitoring program is primarily focused on EROs' adherence with multiple aspects of the Authorized e-file Provider program, such as requirements for Earned Income Tax Credit due diligence, advertising, and electronic signatures. The monitoring program also calls for monitoring of physical information security, which is not required as part of the Authorized e-file Provider program. The Internal Revenue Manual (IRM) details mechanisms and practices for monitoring Authorized e-file Providers, including EROs and online providers.[33] As part of this monitoring, Small Business/Self-Employed (SB/SE) conducts field visits, the number of which more than doubled in the past few years, from almost 300 in 2015 to about 650 in 2018. SB/SE revenue agents visit providers to monitor their operations and to advise providers of any program violations.

IRS uses monitoring visits to investigate allegations, complaints, and warnings against Authorized e-file Providers, as well as to determine

[33]IRM § 4.21.1 *Monitoring the IRS e-file Program* (Aug. 12, 2011).

general compliance with program requirements. While any provider type could undergo a monitoring visit, IRS officials informed us that they primarily conduct field monitoring visits for EROs, which are selected using risk-based criteria. According to these officials, SB/SE coordinates with other IRS offices to provide field monitoring on an as-needed referral basis for other types of Authorized e-file Providers. IRS officials reported that they were unable to confirm the specific number of recent referral monitoring visits but said there were likely fewer than five referrals in the past couple of years.

However, the IRM section detailing the monitoring visits provides little direction for monitoring of information security standards from IRS Publication 1345.[34] The IRM lists monitoring techniques for security, but they focus largely on physical security rather than cybersecurity controls for the electronic aspects of information security. For example, the IRM suggests that agents ask about access to physical files or office keys rather than about how providers send emails containing taxpayer information.

According to our Fraud Risk Framework, agencies should use a risk-based approach to evaluate outcomes and adapt activities to improve fraud risk management.[35] As fraudsters increasingly target paid preparers and tax software providers through cybersecurity attacks, risk-based monitoring and evaluation of cybersecurity controls could help IRS identify fraud risks and potential control deficiencies among third-party providers.

IRS officials said that the SB/SE revenue agents who conduct monitoring visits do not have the technical expertise to effectively monitor information security or cybersecurity controls. For example, an IRS official stated that the IRM monitoring techniques ask about physical security instead of cybersecurity because revenue agents can verify whether filing cabinets are locked or whether computer passwords are visible, but they cannot verify cybersecurity controls, such as whether a provider's information security policies are consistent with government and industry guidelines. Further, an SB/SE official said that, while SB/SE is responsible for monitoring Authorized e-file Providers, cybersecurity is not part of SB/SE's role.

[34]IRM § 4.21.1 *Monitoring the IRS e-file Program* (Aug. 12, 2011).

[35]GAO-15-593SP.

However, we believe there are opportunities for revenue agents to ask basic cybersecurity questions and, at a minimum, use monitoring visits to help promote awareness of leading practices designed to help protect taxpayer information. For example, revenue agents could ask providers if they have secured their office's wireless capabilities, use encryption for sensitive business information, have a designated official in case of a security incident, or know their assigned stakeholder liaison, among other things. Additionally, opportunities exist to leverage resources across IRS to monitor cybersecurity controls. For instance, Cybersecurity has technical expertise that SB/SE could leverage to help monitor these requirements, according to a Cybersecurity official.

Without effective monitoring of information security standards or cybersecurity controls, IRS has limited assurance that EROs' systems are adequately protecting taxpayers' information. If these third parties do not adequately protect that information, taxpayers will face increased risk of both tax-related and non-tax-related identity theft. Improved monitoring could help IRS ensure that it is more effectively detecting and responding to changing fraud risks among providers. Additionally, updating documentation of monitoring activities, as needed, such as the IRM and internal guidance, along with staff training, would provide IRS with better assurance that the greatest risk areas are addressed appropriately.

IRS Does Not Consistently Monitor Authorized e-file Providers' Cybersecurity Controls

IRS conducts limited monitoring of the online provider subset of tax software providers enrolled in the Authorized e-file Provider program. However, these monitoring efforts are not part of the systematic Authorized e-file Provider monitoring program for EROs described above, nor are they documented in the IRM or relevant job aids. According to EPSS officials, IRS does not currently monitor all of the standards for online providers.

IRS staff can remotely monitor three of the six security, privacy, and business standards for online providers through electronic means, according to EPSS officials (see table 3). EPSS officials stated that the other three standards cannot be monitored remotely (see appendix II for the full text of the six security, privacy, and business standards).

Table 3: IRS's Ability to Remotely Monitor Security, Privacy, and Business Standards for Online Providers

Security, privacy, and business standard	Ability to remotely monitor
1. Online providers shall possess a valid and current Extended Validation Secure Sockets Layer certificate using Secure Sockets Layer 3.0 / Transport Layer Security 1.0 or later.	IRS can monitor
2. Online providers shall contract with an independent third-party vendor to run weekly external network vulnerability scans.	IRS cannot monitor
3. Online providers that own or operate a website to collect, transmit, process, or store taxpayer information shall have a written information privacy and safeguard policy consistent with applicable government and industry guidelines. Compliance with these policies shall be certified by a privacy seal vendor acceptable to IRS.	IRS cannot monitor
4. Online providers that own or operate a website to collect, transmit, process, or store taxpayer information shall implement an effective challenge-response protocol (e.g., CAPTCHA) to protect their website against malicious bots.	IRS can monitor
5. Online providers that own or operate a website to collect, transmit, process, or store taxpayer information shall register the website domain's name with a registrar that is in the United States and accredited by the Internet Corporation for Assigned Names and Numbers. The domain name shall be locked and not be private.	IRS can monitor
6. Online providers shall report security incidents to IRS as soon as possible but not later than the next business day after confirmation of the incident.	IRS cannot monitor

Legend: ✔ = IRS can monitor the standard from a remote location such as an IRS office rather than in-person;
✖ = IRS cannot remotely monitor the standard.

Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-19-340

Note: For more information, see Internal Revenue Service, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* Pub. 1345, (Rev. 2-2019)

For two of the three standards that cannot be monitored remotely, EPSS officials said it would be feasible for online providers to send the results of vulnerability scans (standard 2 in table 3) and privacy seal vendor certifications (standard 3 in table 3) to IRS for monitoring purposes.

However, according to these officials, EPSS does not have dedicated staff who could review these results. Similarly, SB/SE, which conducts Authorized e-file Provider monitoring, does not have the technical expertise to review these results, as previously discussed. In addition, IRS cannot monitor the requirement to report security incidents, according to officials, because there is no way for the agency to know whether security incidents have occurred but were not reported. However, every fiscal year, IRS asks online providers to self-certify that they are meeting all six of the security, privacy, and business standards in IRS Publication 1345, according to an EPSS official. To self-certify, providers answer "yes" or "no" questions about whether they have complied with each standard. According to this official, companies generally indicate that they are meeting all of the standards.

In addition to inconsistent monitoring of online provider requirements, IRS has not recently assessed the information security risks among all third-

party provider types. IRS initially implemented the Authorized e-file Provider monitoring program described above only for EROs because they presented the greatest risk for fraud, according to an EPSS official. However, IRS's monitoring practices and the associated IRM section have not been updated since 2011, and still reflect IRS's initial assumption that EROs present the greatest risk for fraud among the different provider types.

Additionally, while IRS assessed the security and privacy risks of tax software providers, the assessment did not compare these risks to those presented by EROs. In 2009, we recommended that IRS assess the extent to which the reliance on tax software creates significant risks to tax administration, including the security and privacy of taxpayer information.[36] IRS agreed with our recommendation and in 2011 received the results of a third-party risk assessment to determine, in part, the security and privacy risks presented by large and small software providers.[37] The assessment found that security presented the biggest overall risk among the areas reviewed—security of information, privacy of information, accuracy of returns, and reliability of systems—due, in part, to security being the least adequately controlled risk area by small software providers. This assessment was not designed to review the risks for other Authorized e-file Provider types, such as EROs.

Our Fraud Risk Framework requires agencies to plan regular fraud risk assessments and suggests tailoring those assessments to the program.[38] Effective managers plan to conduct such assessments at regular intervals and when there are changes to the program or operating environment, such as changes in technology that could result in increased security incidents. As part of a risk assessment, managers may examine the suitability of existing fraud controls. Such examination can help managers identify areas where existing control activities are not suitably designed or implemented to reduce risks to a tolerable level.

By conducting a risk assessment for the Authorized e-file Provider program and identifying the provider types that present the greatest risks

[36]GAO, *Tax Administration: Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks*, GAO-09-297 (Washington, D.C.: Feb. 25, 2009).

[37]This study also determined the security and privacy risks of transmitters, another type of Authorized e-file Provider that sends electronic return data directly to IRS.

[38]GAO-15-593SP.

for fraud, IRS can better determine whether changes to the monitoring program are needed for each provider type. If the agency determines that changes are needed, updating documentation of monitoring activities—such as the IRM, internal guidance, and job aids, along with staff training—would provide IRS with better assurance that the greatest risk areas are addressed appropriately.

IRS Uses Security Incident Information to Protect Taxpayers but Does Not Have a Complete Picture of the Size and Scope of Incidents

IRS Uses Security Incident Reports to Track Taxpayer Accounts and Analyze Trends to Protect Revenue

Multiple offices within IRS use information on security incidents to track trends in fraud schemes, which helps them to protect taxpayer information and to prevent the filing of fraudulent tax returns. For example, when Stakeholder Liaison receives reports about a security incident involving a paid preparer, staff collect additional information about the incident, including the cause of the incident and whether taxpayer information was compromised. Stakeholder Liaison can analyze the data to show geographical information, like the states most affected by breaches; the paid preparer types most affected by incidents; and the method of attack of incidents; among other things, according to a Stakeholder Liaison official. This official said that Stakeholder Liaison also uses this information to produce daily management reports to keep leadership apprised of the number of incidents reported daily, as well as the cumulative number of affected preparers and taxpayers during the year and a comparison to data from the previous year.

Return Integrity and Compliance Services (RICS) officials use a risk-based method to determine the necessary mitigation and treatment plans following a security incident. For example, RICS officials might assess a security incident as high risk, meaning that a taxpayer's personal, financial, and tax data were compromised. For such an incident, RICS officials place the affected Taxpayer Identification Numbers (TIN) on Dynamic Selection Lists—lists of TINs affected in breaches and at risk of

tax-related identity theft—to monitor future tax return filings for potential fraud.[39] On the other hand, for low-risk incidents—incidents where fraudsters may have accessed information like street address or date of birth but not Social Security numbers—RICS may compare victims' current tax returns with prior returns to look for differences that could indicate possible identity theft. According to RICS officials, the office also runs individuals' information through fraud filters to help identify returns with a high likelihood of identity theft.

Criminal Investigation's (CI) Cybercrimes unit shares security incident information with the field offices where the incident occurred, according to CI officials. Area coordinators evaluate the incident information and determine whether a criminal case should be developed. If so, coordinators develop a fraud scheme package and provide it to the agent assigned to the case to help identify other potential incidents resulting from similar schemes, according to CI officials.

IRS May Not Have a Complete Picture of Third-Party Provider Security Incidents Because Its Reporting Requirements Are Not Comprehensive

IRS has primarily tracked information on security incidents in its RICS Incident Management Database since December 2016, according to RICS officials. Security incidents can be categorized in a number of ways, such as when hackers infiltrate third-party providers' systems. Between 2017 and 2018, there was an overall decrease in the number of reported high-risk security incidents that led to confirmed identity theft victims across all types of security incidents. However, the number of reported security incidents from third-party providers increased about 50 percent during this same period, as shown in table 4. In turn, the number of taxpayers affected by the security incidents at third-party providers also increased.

[39]In November 2018, Treasury Inspector General for Tax Administration (TIGTA) reported that RICS analysts did not always add TINs to the Dynamic Selection Lists during the course of their review, as required. The Commissioner of IRS's Wage and Investment Division responded that, as a result, IRS is automating many of the manual processes that caused the issue identified in the report. TIGTA, *Actions Were Not Always Taken to Protect Taxpayers Associated With Reported External Data Breaches*, 2019-40-010 (Washington, D.C.: November 2018).

Table 4: Internal Revenue Service Data on Reported High-Risk Security Incidents, 2017 and 2018

Category	2017	2018
Total number of reported high-risk security incidents	**743**	**523**
Number of reported high-risk security incidents from paid preparers' offices or tax software providers	212	336
Total number of affected taxpayers	**2,275,426**	**933,686**
Number of affected taxpayers from security incidents from paid preparers' offices or tax software providers	180,557	211,162
Total confirmed number of tax-related identity theft victims	**35,070**	**6,774**
Confirmed number of tax-related identity theft victims from security incidents at paid preparers' offices or tax software providers	2,559	3,341

Source: GAO analysis of Internal Revenue Service information. | GAO-19-340

However, IRS does not have comprehensive information about the incidents because, in part, its reporting requirements do not apply to all third-party providers. For example, the Authorized e-file Provider program requires only online providers to report security incidents to IRS as soon as possible but no later than the next business day after confirmation of the incident. The information that online providers are to report includes details about the security incident and the affected taxpayers' accounts.

If paid preparers or EROs experience a security incident at their place of business, they are not required to report any information to IRS about the incident; instead, IRS encourages paid preparers to share security incident information with IRS through Stakeholder Liaison.[40] Additionally, IRS cannot track incidents that third-party providers do not report, according to IRS officials. IRS officials and industry representatives stated that some third-party providers may not report security incidents for fear of punishment from IRS (e.g., penalties, sanctions, or removal from the Authorized e-file Provider program) or negative impacts to their business reputation.[41]

IRS has other voluntary reporting mechanisms for tax software providers or other members of the tax preparation industry. For example, members

[40]Stakeholder Liaison typically takes information about the circumstances of the security incident and information about the affected taxpayers' accounts.

[41]Additional information about the Authorized e-file Provider program and sanctions for violation of program requirements can be found in Department of the Treasury, Internal Revenue Service, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* Pub. 1345 (Rev. 2-2019); and Department of the Treasury, Internal Revenue Service, *IRS* e-file *Application and Participation,* Pub. 3112 (Rev. 7-2018).

of the Security Summit can use a voluntary reporting mechanism to submit information to RICS. Some members of the Security Summit can use an additional voluntary reporting system in the ISAC online platform, which sends alerts about security incidents to others in the platform.

IRS also recently revised some of its requirements that could affect paid preparers' reporting of security incidents while using other IRS services. For example, in October 2018, the agency updated its user agreement for e-Services, a suite of web-based tools that allow paid preparers, among others, to complete transactions online with IRS.[42] This update included a requirement to report any unauthorized use of the e-Services account or any other breach of security as soon as users become aware of the incident.[43]

According to Internal Control Standards, agencies should use quality information, both internal and external, to achieve objectives. For example, agencies should obtain data on a timely basis so that they can be used for effective monitoring.[44] Additionally, recommended controls in NIST Special Publication 800-53 require reporting of suspected security incidents by federal agencies and their subordinate organizations.

Though IRS conducts a yearly review of requirements for Authorized e-file Providers to find needed updates, the incident reporting requirement has not been identified as needing updates since 2010, according to a senior Wage and Investment official. This is another instance where centralized leadership could have identified a need to update the incident reporting requirements.

According to an EPSS official, IRS originally applied this incident reporting requirement to only online providers because these providers stored a large amount of data and carried the highest risk of data loss. Similarly, IRS officials said the reporting requirement for online providers does not apply to providers of tax software used by paid preparers

[42]e-Services is a suite of web-based tools that allow tax professionals like paid preparers, reporting agents, mortgage professionals, taxpayers, and others to complete transactions online with IRS.

[43]Similarly, e-Services users who use an intermediate service provider to obtain information from e-Services must report vulnerabilities, breaches, or compromised e-Services accounts to IRS within 1 business day of the discovery. The user agreement states that these users may also report the incident to Stakeholder Liaison.

[44]GAO-14-704G.

because those software providers do not collect or store taxpayer information on their systems. Instead, the taxpayer information is stored on a paid preparer's hard drive. If a security incident occurred at the business of a paid preparer who uses tax software, then the preparer, not the tax software provider, would report that incident to IRS, according to IRS officials.

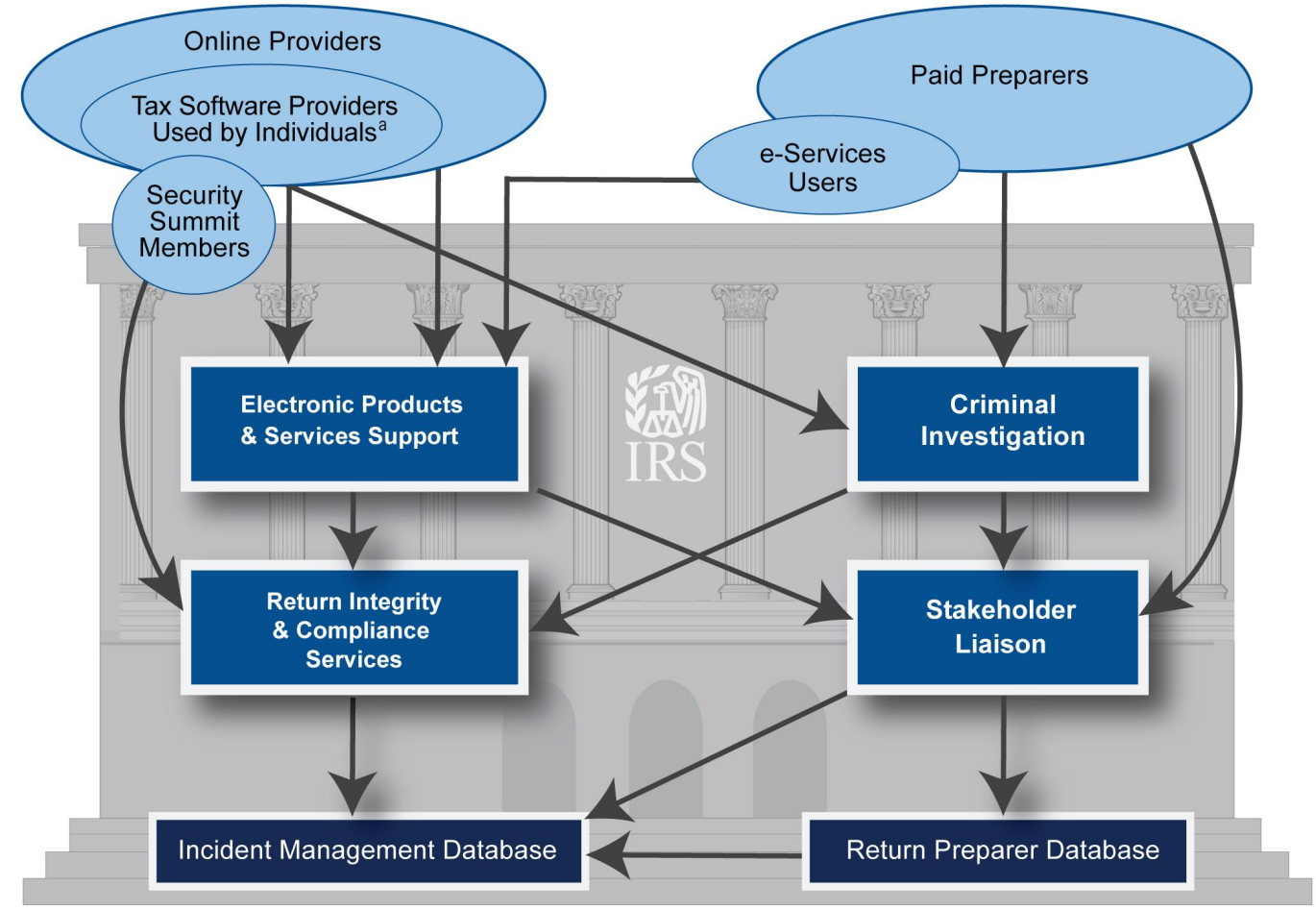
While voluntary reporting mechanisms and updating of user agreements for IRS's website are important steps, without a clear and standardized reporting requirement for all types of providers, IRS will not have assurance that third-party providers consistently report their security incidents in a timely manner. IRS needs this information to better understand the size and scope of information security incidents, which it uses to protect compromised individual taxpayer accounts and prevent identity theft refund fraud.

IRS Has Not Documented Processes for Third-Party Provider Security Incident Reporting or Data Storage

Security incident information can be reported to IRS through various channels from the public to IRS offices, and the data are ultimately stored in the RICS Incident Management Database regardless of the office that initially received the information. Figure 5 depicts the flow of information from the public to IRS offices, as well as the flow of information between the offices and to IRS databases.[45]

[45]Not all offices depicted previously in figure 3 receive security incident information from the public.

Figure 5: IRS Has Complex Processes for the Intake, Sharing, and Storage of Security Incident Information



Source: GAO analysis of IRS data processes. I GAO-19-340

Notes: Ovals showing information sources are not proportional and do not represent the number of paid preparers, tax software providers, or other populations.

The graphic shows the general flow of security incident data to the two main incident tracking databases, the Incident Management Database and the Return Preparer Database. The graphic does not show all communication, coordination, or information sharing among offices.

[a]Incidents involving tax software used by paid preparers would be reported to IRS by the paid preparers rather than the tax software provider.

While RICS has documented its information intake, tracking, and storage processes in the RICS Incident Management Plan, IRS does not have a comprehensive document that describes these processes across the different IRS offices. For example, incident information submitted to EPSS and Stakeholder Liaison eventually moves to RICS to be tracked in the Incident Management Database. Additionally, RICS officials told us that they track each of these reported incidents separately and that the main repository should not contain duplicate reports of the same incidents, though multiple databases may contain information about the same incident. RICS officials added that, before a new incident is added to the Incident Management Database, staff conduct a query in the database to ensure that the incident was not already added. However, IRS has not documented how the security incident data processes should flow, relying instead on informal communication efforts of the staff and the assumption that staff know where the data belong and will provide that information to the appropriate offices.

Internal Control Standards state that management should develop and maintain documentation of its internal control system and implement control activities through policies.[46] The standards also state that documentation of responsibilities through policies and periodic review of activities can contribute to the effectiveness of implementation.

This limited nature of the documentation may be due to the newness of some of these data processes. For example, a Stakeholder Liaison official told us that the data intake process for Stakeholder Liaison and entry into the Return Preparers Database started at the beginning of 2018. Prior to that, a Stakeholder Liaison manager stored information about security incidents in an individual email account because there was no mechanism for storing the data in a systematic manner. Further, a senior Wage and Investment Division official stated that the processes to intake, store, and share the data among the different IRS offices continue to evolve, and that documents describing these practices may quickly become obsolete.

While these processes may still be evolving, documenting them can help IRS combat identity theft by helping to ensure that security incidents are properly recorded and monitored in the IRS systems. Documenting the processes may also allow for more complete data, as the data would

[46]GAO-14-704G.

follow a specific routing and review process. This would reduce the risk of the data not following the various channels they go through now. Such documentation can also help IRS retain organizational knowledge, mitigate the risk of having that knowledge limited to a few personnel, and ensure that the agency implements these processes effectively in the future.

Conclusions

Tens of millions of taxpayers use third-party providers, such as paid preparers or tax software providers, to comply with their federal income tax obligations. It is critical that taxpayers' information, which includes personally identifiable and other sensitive information, be kept secure to maintain public confidence and avoid data breaches that expose that information for use by fraudsters. Identity theft is a constantly evolving crime, but IRS's information security standards for third-party providers' systems have not kept pace with the changing environment. One reason for this is that IRS lacks the explicit authority to require minimum standards for the systems of paid preparers and Authorized e-file Providers. Without this authority, Congress and IRS have limited assurance that the processes used to collect, store, and submit taxpayers' returns adequately protect taxpayers' information against electronic data breaches and potential tax refund fraud.

Modifying its Authorized e-file Provider program requirements to explicitly state the elements of an information security program as required under the FTC Safeguards Rule would help IRS ensure that Authorized e-file Providers are aware of, and comply with, the rule. Doing so could also help these providers better protect taxpayers' information. Additionally, IRS is missing an opportunity to capitalize on the achievements of Security Summit members to help ensure that tax software providers have an equivalent level of standards in place to adequately protect taxpayer information.

The lack of centralized leadership at IRS with responsibility for coordinating all aspects of protecting taxpayer information held by third-party providers has enabled missed opportunities. Such designated leadership could help ensure greater collaboration between the various IRS offices that have roles to play in this area. This leadership could have also ensured that security standards for online providers in the Authorized e-file Provider program would have been updated. Instead, IRS

introduced these standards in 2010 and has not subsequently updated them.

Incorporating cybersecurity into its monitoring visits for EROs would provide IRS with greater assurance that EROs' systems are adequately protecting taxpayers' information from an increased risk of both tax-related and non-tax-related identity theft. Further, ensuring that IRS is using a risk-based approach to review all types of Authorized e-file Providers would provide assurance that the greatest risk areas of fraud are addressed appropriately.

Finally, IRS's efforts to protect taxpayer information at third-party providers would also be strengthened by greater consistency in requirements across provider types for reporting security incidents. Greater consistency would help to ensure IRS is obtaining timely and reliable information from third-party providers so IRS can better understand the size and scope of security incidents—data it uses to protect compromised individual taxpayer accounts and prevent identity theft refund fraud. Documenting the intake, storage, and sharing of the security incident data would also help IRS ensure that the security incidents are properly recorded and monitored.

Matter for Congressional Consideration

Congress should consider providing IRS with explicit authority to establish security requirements for the information systems of paid preparers and Authorized e-file Providers. (Matter for Consideration 1)

Recommendations for Executive Action

We are making the following eight recommendations to IRS.

The Commissioner of Internal Revenue should develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers. (Recommendation 1)

The Commissioner of Internal Revenue should modify the Authorized e-file Provider program's requirements to explicitly state the required elements of an information security program as provided by the FTC Safeguards Rule. (Recommendation 2)

The Commissioner of Internal Revenue should require that all tax software providers that participate in the Authorized e-file Provider program follow the subset of NIST Special Publication 800-53 controls that were agreed upon by the Security Summit participants. (Recommendation 3)

The Commissioner of Internal Revenue should regularly review and update the security requirements that apply to tax software providers and other Authorized e-file Providers. (Recommendation 4)

The Commissioner of Internal Revenue should update IRS's monitoring programs for electronic return originators to include techniques to monitor basic information security and cybersecurity issues. Further, IRS should make the appropriate revisions to internal guidance, job aids, and staff training, as necessary. (Recommendation 5)

The Commissioner of Internal Revenue should conduct a risk assessment to determine whether different monitoring approaches are appropriate for all of the provider types in the IRS's Authorized e-file Provider program. If changes are needed, IRS should make appropriate revisions to the monitoring program, internal guidance, job aids, and staff training, as necessary. (Recommendation 6)

The Commissioner of Internal Revenue should standardize the incident reporting requirements for all types Authorized e-file Providers. (Recommendation 7)

The Commissioner of Internal Revenue should document intake, storage, and sharing of the security incident data across IRS offices. (Recommendation 8)

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 three of the recommendations and disagreed with five of the recommendations. IRS also provided technical comments, which we incorporated as appropriate.

IRS agreed with our recommendations to regularly review and update the security requirements that apply to the tax software provider and other

Authorized e-file Providers; standardize the incident reporting requirements for all types of Authorized e-file Providers; and document intake, storage, and sharing of the security incident data across IRS offices. IRS did not provide additional detail on the actions it plans to take to address these recommendations.

IRS disagreed with five of our recommendations, generally citing for all of them the lack of clear and explicit authority it would need to establish security requirements for the information systems of paid preparers and others who electronically file returns.

For our recommendation to develop a governance structure or other form of centralized leadership, IRS stated it would require statutory authority that clearly communicates its authority to establish security requirements for the information systems of paid preparers and others who electronically file tax returns. Further, IRS stated that without such authority, implementing the recommendation would be an inefficient, ineffective, and costly use of resources. We disagree that convening a governance structure or other centralized form of leadership would require additional statutory authority or be inefficient, ineffective, and costly. As discussed in the report, IRS has seven different offices across the agency working on information security-related activities that could benefit from centralized oversight and coordination, such as updating existing standards, monitoring Authorized e-file Provider program compliance, and tracking security incident reports.

We continue to believe that establishing a governance structure would help provide this level of leadership, coordination, and collaboration to IRS's current efforts and therefore help alleviate the missed opportunities that we identified in the report, such as updating outdated security standards. Further, IRS could choose a leadership mechanism that it determines to be low cost and most efficient to gain a higher degree of coordination. Without this structure, it is unclear how IRS will adapt to changing security threats in the future and ensure those threats are mitigated.

In our draft report, we made a recommendation that IRS modify the Authorized e-file Provider program to be consistent with the FTC Safeguards Rule. In its response, IRS stated that it did not have explicit authority to establish policy consistent with the FTC Safeguards Rule or enforce compliance with it. However, IRS clearly states in its Revenue Procedure 2007-40 that violations of the provisions of the Gramm-Leach-Bliley Act and the implementing rules and regulations promulgated by

FTC are considered violations of the revenue procedure and may subject an Authorized e-file Provider to penalties or sanctions. Therefore, we believe IRS has already incorporated compliance with the FTC Safeguards Rule as part of its Authorized e-file Provider program.

The intent of this recommendation is not to suggest that IRS develop new policies related to the elements of the Safeguards Rule. Instead, we believe IRS has the opportunity to explicitly state in its requirements for Authorized e-file Providers the elements of an information security program, as listed in the Safeguards Rule. This action will help third party providers become aware of their specific legal obligations to protect taxpayer data under the Gramm-Leach-Bliley Act. As such, we clarified text in the body of the report and the text of the recommendation to better reflect our intent.

For our recommendation to require all tax software providers that participate in the Authorized e-file Provider program to follow the subset of NIST Special Publication 800-53 controls that were agreed upon by the Security Summit participants, IRS stated that it does not have the statutory authority for such a requirement. However, under its existing authority, IRS has already established some information security requirements for a portion of tax software providers—those that are online providers. IRS has the opportunity to further establish standards for all tax software providers by incorporating the subset of NIST controls into its Authorized e-file Provider program, which would capitalize on the work it has completed with the Security Summit members. We continue to believe that without setting and requiring the same security standards for all tax software providers, IRS does not have assurance that these providers have an equivalent level of standards in place to adequately protect taxpayer information.

For our recommendation that IRS update its monitoring programs for electronic return originators, IRS stated it does not have the statutory authority to establish policy on information security and cybersecurity issues, nor to enforce compliance if noncompliance is observed. However, as we reported, IRS already monitors physical aspects of information security, which goes beyond existing Authorized e-file Provider program requirements. Since most individuals now file tax returns electronically, having checks for physical security without comparable checks for cybersecurity does not address current risks, as cyber criminals and fraudsters are increasingly attacking third-party providers, as IRS has noted. We believe that incorporating some basic cybersecurity monitoring into the visits would provide IRS the opportunity

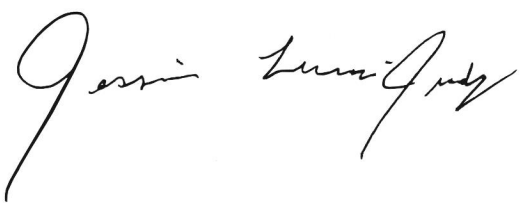
to help inform the most vulnerable third-party providers of additional guidance and resources.

For our recommendation to conduct a risk assessment to determine whether different monitoring approaches are appropriate for all of the provider types in the Authorized e-file Provider program, IRS stated that changes to the monitoring program would not have value to the overall program performance absent statutory authority. We disagree with this conclusion. As discussed in the report, IRS does not currently systematically monitor the existing security requirements for online providers, nor does it conduct information security or cybersecurity monitoring for all types of Authorized e-file Providers. We believe that IRS could conduct a risk assessment of its current monitoring program within existing statutory authority and make necessary changes that would provide better assurance that all types of providers are receiving some level of oversight and that IRS is addressing the greatest risk areas appropriately.

We are sending 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 are also sending 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 have any questions about this report, please contact me at (202) 512-9110 or Lucasjudyj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,



Jessica Lucas-Judy
Director, Tax Issues
Strategic Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) assess what is known about the taxpayer information security requirements for the systems used by third-party providers, (2) describe Internal Revenue Service's (IRS) outreach efforts to third-party providers on the requirements, (3) assess IRS's monitoring processes for ensuring third-party providers' compliance with the requirements, and (4) assess IRS's requirements for third-party provider security incident reporting and how IRS uses that information.

To assess what is known about the taxpayer information security requirements for the systems used by third-party providers, such as paid preparers and tax software providers, we reviewed applicable laws and regulations such as the Gramm-Leach-Bliley Act and relevant portions of the Internal Revenue Code, including 26 U.S.C. § 6011.[1] This section of the Internal Revenue Code prescribes the filing of income tax returns, as well as the electronic filing requirements for returns prepared by paid preparers. We reviewed 26 U.S.C. §7803, which provides that the IRS Commissioner has the authority to administer and manage the execution and application of tax laws, while balancing the rights of, among other things, confidentiality and privacy of the taxpayer. We also reviewed the Federal Trade Commission's (FTC) Safeguards Rule, which requires financial institutions, including tax return preparers, affiliates, and service providers, to ensure the security and confidentiality of customer records and information.[2] This rule applies to those who are significantly engaged in providing financial products or services that include preparation and filing of tax returns. We reviewed IRS Revenue Procedure 2007-40, which informs Authorized e-file Providers of their obligations to IRS, taxpayers, and other participants in the Authorized e-file Provider program and outlines the rules governing filing electronically with IRS.

We reviewed IRS publications describing the obligations in IRS's Revenue Procedure 2007-40 and the requirements of the Authorized e-

[1]Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999), *codified at* 15 U.S.C. §§ 6801–6827 (Nov. 12, 1999); 26 U.S.C. § 6011.

[2]FTC Safeguards Rule, 16 C.F.R. Part 314.

file Provider program, including IRS Publication 3112, *IRS e-file Application and Participation*, and IRS Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.* We assessed these documents to determine if the requirements for third-party providers were incorporating the laws and following leading practices as outlined by *Standards for Internal Control in the Federal Government* (Internal Control Standards) and *A Framework for Managing Fraud Risk in Federal Programs* (Fraud Risk Framework).[3] The Fraud Reduction and Data Analytics Act of 2015, and Office of Management and Budget guidance implementing its provisions, affirm that agencies should adhere to the leading practices identified in our Fraud Risk Framework.[4] We also compared the standards published in Publication 1345 for online providers to the National Institute of Standards and Technology (NIST) Special Publication 800-52: *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* to determine if the standards were following leading practices.[5] We reviewed the subset of NIST Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations* controls that the Security Summit members agreed to voluntarily implement.[6]

We also reviewed other IRS publications that provide third-party providers with descriptions of leading practices in keeping taxpayer information safe, including IRS Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business;* IRS Publication 4600, *Tips for Safeguarding Taxpayer Data*; IRS Publication 5293, *Protect Your Clients; Protect Yourself: Data Security Resource Guide for Tax Professionals*; and IRS Publication 5294, Protect Your Clients; Protect Yourself: Data Security Tips for Tax Professionals. In assessing these documents, we identified

[3]GAO, *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 28, 2015); and *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[4]Pub. L. No. 114-186, § 3, 130 Stat. 546, 546-47 (June 30, 2016); Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (Washington, D.C.: July 15, 2016).

[5]National Institute of Standards and Technology, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, Special Publication 800-52, Revision 1 (Gaithersburg, Md.: April 2014).

[6]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

the extent of consistency among publications. We interviewed IRS officials who were responsible for various aspects of IRS's security requirements for paid preparers and tax software providers.

We conducted semistructured interviews with the following 10 industry groups and related organizations that represented a cross section of the tax preparation industry to determine their knowledge about existing information security requirements.

- American Bar Association
- American Coalition for Taxpayer Rights
- American Institute of Certified Public Accountants
- American Payroll Association
- Council for Electronic Revenue Communication Advancement
- Cyber Threat Alliance
- Electronic Tax Administration Advisory Committee
- Federation of Tax Administrators
- National Association of Tax Professionals
- National Society of Tax Professionals

We reviewed IRS organization documents, including organizational charts and associated Internal Revenue Manual (IRM) provisions for the offices that have responsibilities for securing taxpayer information.[7] We reviewed the stated missions of the offices of Electronic Products and Services Support (EPSS); Small Business/Self-Employed; Return Integrity and Compliance Services (RICS); Criminal Investigation (CI); Return Preparer Office; Office of Professional Responsibility; Cybersecurity; and Stakeholder Liaison. We also interviewed officials from these offices to determine how they coordinated the responsibilities for overseeing the security of taxpayer data among the offices. We compared IRS activities to the Internal Control Standards that identify controls that help an entity adapt to shifting environments, evolving demands, changing risks, and new priorities.

[7]The IRM is IRS's primary, official compilation of instructions to staff that relate to the administration and operations of the IRS. IRM § 1.11.2 *Internal Revenue Manual (IRM) Process* (Oct. 11, 2018).

To describe the outreach efforts IRS takes for third-party providers, we reviewed IRS outreach documents such as publications, news releases, social media posts, emails, webinars, and online education campaigns. We interviewed IRS officials and conducted semistructured interviews with 10 industry groups and related organizations to determine IRS's communication efforts related to security standard enforcement and identify potential challenges that IRS faces in its outreach.

To assess IRS's monitoring processes for ensuring third-party providers' compliance with information security requirements, we reviewed the agency's monitoring procedures for the Authorized e-file Provider program per Rev. Proc. 2007- 40; IRS Publication 3112, *IRS e-file Application and Participation;* and IRS Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.* We reviewed the IRM section related to Monitoring the IRS e-file Program, monitoring checklists, and related job aides to determine the extent to which monitoring practices address security requirements in IRS Publication 1345.[8] We assessed IRS's monitoring efforts against our Fraud Risk Framework's principles to combat fraud in a strategic, risk-based manner.[9] We also interviewed the IRS officials responsible for overseeing the monitoring program.

To assess IRS's requirements for third-party provider reporting of security incidents and how IRS uses that information, we reviewed IRS guidance about security incident reporting requirements. We analyzed IRS data on the number and type of security incidents tracked in the RICS Incident Management Database from 2017 and 2018, the only data available following its creation in December 2016. We interviewed RICS officials about the quality of data in this database and determined that the data were sufficiently reliable to describe a minimum count of security incidents. Specifically, we asked about the responsibilities of officials collecting and using the data, the procedures in place to capture all reported data, and controls for ensuring the accuracy of the data and resolving any errors, among other things. We reviewed IRS guidance and program user agreements to determine security incident reporting requirements for third-party providers. We reviewed IRS process documentation and interviewed IRS officials from EPSS, RICS, CI, Return Preparer Office, Cybersecurity, and Stakeholder Liaison to determine the

[8]IRM Part 4, Chapter 21, Sec. 1.

[9]GAO-15-593SP

collection, routing, and storage processes for security incident information. We assessed IRS's processes and documentation practices against leading practices outlined in NIST Special Publication 800-53 and Internal Control Standards.[10] We interviewed IRS officials to identify ways that IRS uses this security incident information. We conducted semistructured interviews with the 10 industry groups and related organizations listed above to determine their knowledge about existing security incident reporting requirements.

We conducted this performance audit from November 2017 to May 2019 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.

[10]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

Appendix II: Security and Privacy Standards for Online Providers

The Internal Revenue Service (IRS) mandated that online providers adhere to six privacy, security, and business standards as part of the Authorized e-file Provider program, as listed in table 6. These standards have not been updated since they were developed in 2010.

Table 5: IRS's Security, Privacy, and Business Standards for Online Providers

Standards for Online Providers
1. Extended Validation Secure Sockets Layer Certificate Online Providers of individual income tax returns shall possess a valid and current Extended Validation Secure Sockets Layer certificate using SSL 3.0 / TLS 1.0 or later and minimum 1024-bit RSA / 128-bit AES.
2. External Vulnerability Scan Online Providers of individual income tax returns shall contract with an independent third-party vendor to run weekly external network vulnerability scans of all their "system components" in accordance with the applicable requirements of the Payment Card Industry Data Security Standards. All scans shall be performed by a scanning vendor certified by the Payment Card Industry Security Standards Council and listed on their current list of Approved Scanning Vendors. In addition, Online Providers of individual income tax returns whose systems are hosted shall ensure that their host complies with all applicable requirements of the Payment Card Industry Data Security Standards. For the purposes of this standard, "system components" is defined as any network component, server, or application that is included in or connected to the taxpayer data environment. The taxpayer data environment is that part of the network that possesses taxpayer data or sensitive authentication data. If scan reports reveal vulnerabilities, action shall be taken to address the vulnerabilities in line with the scan report's recommendations. Retain weekly scan reports for at least one year. The Approved Scanning Vendor and the host (if present) shall be in the United States.
3. Information Privacy and Safeguard Policies This standard applies to Authorized IRS e-file Providers participating in Online Filing of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed, or stored. These Providers shall have a written information privacy and safeguard policy consistent with the applicable government and industry guidelines and including the following statement: "We maintain physical, electronic and procedural safeguards that comply with applicable law and federal standards." In addition, Providers' compliance with these policies shall be certified by a privacy seal vendor acceptable to IRS.
4. Website Challenge-Response Test This standard applies to Providers participating in Online Filing of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed, or stored. These Providers shall implement an effective challenge-response protocol (e.g., CAPTCHA) to protect their website against malicious bots. Taxpayer information shall not be collected, transmitted, processed, or stored unless the user successfully completes this challenge-response test.

Standards for Online Providers
5. Public Domain Name Registration This standard applies to Online Providers of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed, or stored. These Online Providers shall have their website's domain name registered with a domain name registrar that is in the United States and accredited by the Internet Corporation for Assigned Names and Numbers. The domain name shall be locked and not be private.
6. Reporting of Security Incidents Online Providers of individual income tax returns shall report security incidents to IRS as soon as possible but not later than the next business day after confirmation of the incident. For the purposes of this standard, an event that can result in an unauthorized disclosure, misuse, modification, or destruction of taxpayer information shall be considered a reportable security incident. See instructions for submitting incident reports. In addition, if the Online Provider's website is the proximate cause of the incident, the Online Provider shall cease collecting taxpayer information via their website immediately upon detection of the incident and until the underlying causes of the incident are successfully resolved.

Source: Internal Revenue Service (IRS) information. | GAO-19-340

Note: For more information, see Internal Revenue Service Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns, Pub. 1345, (Rev. 2-2019).

Appendix III: Comments from the Internal Revenue Service

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

DEPUTY COMMISSIONER

April 12, 2019

Ms. Jessica Lucas-Judy
Director, Tax Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Lucas-Judy:

I have reviewed the draft report entitled *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices* (GAO-19-340) and appreciate the opportunity to provide comments. It is important to note that the IRS does not endorse or promote tax return preparers or tax return preparation software products. The selection of these services and service providers are made by individuals and businesses as consumers outside the arena of tax administration. The IRS establishes criteria for tax return preparation software and transmission systems to ensure their ability to interface with IRS systems, and we establish criteria for participation in the IRS e-file program. However, the IRS does not have the statutory authority to establish data security requirements and enforce compliance with those requirements on third-party transactions or relationships.

As the GAO concludes in the report, the IRS has not been given the explicit authority to establish and require minimum data security standards for the systems of paid return preparers and other parties involved in the electronic filing process. We agree with this conclusion and further submit that, should such authority be provided, a commensurate level of funding is also required to ensure our ability to enforce compliance with the data security standards.

We disagree with the GAO's conclusion that a lack of centralized leadership contributes to missed opportunities for ensuring that third-party providers adequately protect taxpayers' information. Tax-related identity theft affects taxpayers in different ways, depending on the type and amount of personally identifiable information an identity thief has obtained and how they use that data. Different treatment streams are required to proactively detect and stop potential victimization than those used when victimization has been discovered after the fact. Multiple functions within the IRS provide specialized treatments based on the nature of the identity theft fraud; however, those functions

constantly communicate with one another to ensure the overall identity theft strategy is effective. Should authority and funding be granted, there would be an opportunity to identify and evaluate opportunities for efficiencies to be gained from centralized administration of the electronic tax return preparation and filing processes from both the consumer transaction and tax administration aspects.

The preventive measures and victim assistance processes we have developed were designed and operate under the tax administration authority the Congress has granted to the IRS. With these processes, we have caused significant annual decreases in the amount of attempted and estimated undetected identity theft-related refund fraud. Estimated identity theft attempted in 2012 was approximately $31 billion, with $9.4 billion estimated as being undetected, or not prevented[1]. By 2017, estimated attempted identity theft-related refund fraud declined to an approximated average of $12.15 billion, with an average $11.8 billion detected and stopped, and an estimated average of $360 million undetected and not stopped. The Identity Theft Taxonomy methodology has been reviewed by both the GAO and the Treasury Inspector General for Tax Administration and is an accurate estimation of the scope and impact of identity theft on the tax system, and reflective of the results of our actions to combat refund fraud attributed to identity theft.

The report recommends actions that we would consider, given the appropriate statutory authority and funding; however, lacking those fundamental needs, we do not agree to the recommendations that would cause the IRS to exceed its authority by overreaching into the realm of commercial relationships. We do agree to update our publications and recommended guidance to participants within the e-file program.

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

Sincerely,

Kirsten B. Wielobob
Deputy Commissioner for
Services and Enforcement

Enclosure

[1] IRS Taxonomy, Identity Theft Protected v. Unprotected Estimates 2012 – 2017.

Enclosure

Recommendations for Executive Action

Recommendation 1
The Commissioner of Internal Revenue should develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers.

Comment
We disagree with this recommendation. As recognized by the GAO, the IRS does not have clear and explicit authority to establish security requirements for the information systems of paid preparers and others who electronically file returns. To effectively establish data safeguarding policies and implement strategies enforcing compliance with those policies, a centralized leadership structure requires the statutory authority that clearly communicates the authority of the IRS to do so. Without such authority, implementing the recommendation would be an inefficient, ineffective, and costly use of resources.

Recommendation 2
The Commissioner of Internal Revenue should modify the Authorized e-file Provider program to be consistent with the FTC Safeguards Rule.

Comment
We disagree with this recommendation. The IRS does not have explicit authority to establish policy consistent with the Federal Trade Commission's Safeguards Rule or enforce compliance with it.

Recommendation 3
The Commissioner of Internal Revenue should require that all tax software providers that participate in the Authorized e-file Provider program follow the subset of National Institute of Standards and Technology (NIST) Special Publication 800-53 controls that were agreed upon by the Security Summit participants.

Comment
We disagree with this recommendation. The IRS does not have the statutory authority to require Authorized e-file Provider program participants to comply with the NIST Special Publication 800-53.

Recommendation 4
The Commissioner of Internal Revenue should regularly review and update the security requirements that apply to tax software providers and other Authorized e-file Providers.

Comment
We agree with this recommendation.

Recommendation 5
The Commissioner of Internal Revenue should update IRS's monitoring programs for electronic return originators to include techniques to monitor basic information security and cybersecurity issues. Further, IRS should make the appropriate revisions to internal guidance, job aids, and staff training, as necessary.

Comment
We disagree with this recommendation. The IRS does not have the statutory authority to establish policy on information security and cybersecurity issues, nor to enforce compliance if non-compliance is observed. Additionally, the specialized technical skills required to monitor compliance with information and cybersecurity standards, should statutory authority be granted, would require additional funding to meet those monitoring needs.

Recommendation 6
The Commissioner of Internal Revenue should conduct a risk assessment to determine whether different monitoring approaches are appropriate for all of the provider types in the IRS's Authorized e-file Provider program. If changes are needed, IRS should make appropriate revisions to the monitoring program, internal guidance, job aids, and staff training, as necessary.

Comment
We disagree with this recommendation. Absent requisite statutory authority and funding, changes in the monitoring program, internal guidance, job aids, and staff training will not have value to the overall program performance.

Recommendation 7
The Commissioner of Internal Revenue should standardize the incident reporting requirements for all types Authorized e-file Providers.

Comment
We agree with this recommendation.

Recommendation 8
The Commissioner of Internal Revenue should document intake, storage, and sharing of the security incident data across IRS offices.

Comment
We agree with this recommendation.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Jessica Lucas-Judy, (202) 512-9110 or LucasJudyJ@gao.gov

Staff Acknowledgements

In addition to the contact named above, Jeff Arkin (Assistant Director), Robyn Trotter (Analyst-in-Charge), Christina Bixby, Alyssia Borsella, Mark Canter, Jehan Chase, Larry Crosland, Ann Czapiewski, James Andrew Howard, Michele Fejfar, and Robert Gebhart made key contributions to this report.

Appendix V: Accessible Data

Data Tables

Accessible Data for How Individual Tax Returns Were Filed, Calendar Year 2018

Category	Percentage	Number
Paper filed by paid preparers	3 %	3.9 million
Paper filed by taxpayer	7%	11.1 million
Electronically filed by taxpayer	37%	55.2 million
Electronically filed by paid preparer	53%	80.3 million

Accessible Data for Figure 2: How Individual Income Tax Returns Were Filed, 2018

Category	Percentage	Number
Paper filed by paid preparers	3 %	3.9 million
Paper filed by taxpayer	7 %	11.1 million
Electronically filed by taxpayer	37%	55.2 million
Electronically filed by paid preparer	53%	80.3 million

Agency Comment Letter

Accessible Text for Appendix III Comments from the Internal Revenue Service

Page 1

April 12, 2019

Ms. Jessica Lucas-Judy

Director, Tax Issues

U.S. Government Accountability Office

441 G Street, N.W.

Washington, DC 20548

Dear Ms. Lucas-Judy:

I have reviewed the draft report entitled Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices (GAO-19-340) and appreciate the opportunity to provide comments. It is important to note that the IRS does not endorse or promote tax return preparers or tax return preparation software products. The selection of these services and service providers are made by individuals and businesses as consumers outside the arena of tax administration. The IRS establishes criteria for tax return preparation software and transmission systems to ensure their ability to interface with IRS systems, and we establish criteria for participation in the IRS e-file program. However, the IRS does not have the statutory authority to establish data security requirements and enforce compliance with those requirements on third-party transactions or relationships.

As the GAO concludes in the report, the IRS has not been given the explicit authority to establish and require minimum data security standards for the systems of paid return preparers and other parties involved in the electronic filing process. We agree with this conclusion and further submit that, should such authority be provided, a commensurate level of funding Is also required to ensure our ability to enforce compliance with the data security standards.

We disagree with the GAO's conclusion that a lack of centralized leadership contributes to missed opportunities for ensuring that third-party providers adequately protect taxpayers' information. Tax-related identity theft affects taxpayers in different ways, depending on the type and amount of personally identifiable information an identity thief has obtained and how they use that data. Different treatment streams are required to proactively detect and stop potential victimization than those used when victimization has been discovered after the fact. Multiple functions within the IRS provide specialized treatments based on the nature of the identity theft fraud; however, those functions

constantly communicate with one another to ensure the overall identity theft strategy is effective. Should authority and funding be granted, there would be an opportunity to identify and evaluate opportunities for efficiencies to be gained from centralized administration of the electronic tax return preparation and filing processes from both the consumer transaction and tax administration aspects.

The preventive measures and victim assistance processes we have developed were designed and operate under the tax administration authority the Congress has granted to the IRS. With these processes, we have caused significant annual decreases in the amount of attempted and estimated undetected identity theft-related refund fraud. Estimated identity theft attempted in 2012 was approximately $31 billion, with $9.4 billion estimated as being undetected, or not prevented1• By 2017, estimated attempted identity theft-related refund fraud declined to an approximated average of $12.15 billion, with an average $11.8 billion detected and stopped, and an estimated average of $360 million undetected and not stopped. The Identity Theft Taxonomy methodology has been reviewed by both the GAO and the Treasury Inspector General for Tax Administration and is an accurate estimation of the scope and impact of identity theft on the tax system, and reflective of the results of our actions to combat refund fraud attributed to identity theft.

The report recommends actions that we would consider, given the appropriate statutory authority and funding; however, lacking those fundamental needs, we do not agree to the recommendations that would cause the IRS to exceed its authority by overreaching into the realm of commercial relationships. We do agree to update our publications and recommended guidance to participants within thee-file program.

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

Sincerely,

Kirsten B. Wielobob

Deputy Commissioner for Services and Enforcement

Enclosure

[1] IRS Taxonomy, Identity Theft Protected v. Unprotected Estimates 2012- 2017.

Page 3

Recommendations for Executive Action

Recommendation 1

The Commissioner of Internal Revenue should develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers.

Comment

We disagree with this recommendation. As recognized by the GAO, the IRS does not have clear and explicit authority to establish security requirements for the information systems of paid preparers and others who electronically file returns. To effectively establish data safeguarding policies and implement strategies enforcing compliance with those policies, a centralized leadership structure requires the statutory authority that clearly communicates the authority of the IRS to do so. Without such authority, implementing the recommendation would be an inefficient, ineffective, and costly use of resources.

Recommendation 2

The Commissioner of Internal Revenue should modify the Authorized e-file Provider program to be consistent with the FTC Safeguards Rule.

Comment

We disagree with this recommendation. The IRS does not have explicit authority to establish policy consistent with the Federal Trade Commission’s Safeguards Rule or enforce compliance with it.

Recommendation 3

The Commissioner of Internal Revenue should require that all tax software providers that participate in the Authorized e-file Provider program follow the subset of National Institute of Standards and

Technology (NIST) Special Publication 800-53 controls that were agreed upon by the Security Summit participants.

Comment

We disagree with this recommendation. The IRS does not have the statutory authority to require Authorized e-file Provider program participants to comply with the NIST Special Publication 800-53.

Recommendation 4

The Commissioner of Internal Revenue should regularly review and update the security requirements that apply to tax software providers and other Authorized e-file Providers.

Comment

We agree with this recommendation.

Page 4

Recommendation 5

The Commissioner of Internal Revenue should update IRS's monitoring programs for electronic return originators to include techniques to monitor basic information security and cybersecurity issues. Further, IRS should make the appropriate revisions to internal guidance, job aids, and staff training, as necessary.

Comment

We disagree with this recommendation. The IRS does not have the statutory authority to establish policy on information security and cybersecurity issues, nor to enforce compliance if non-compliance is observed. Additionally, the specialized technical skills required to monitor compliance with information and cybersecurity standards, should statutory authority be granted, would require additional funding to meet those monitoring needs.

Recommendation 6

The Commissioner of Internal Revenue should conduct a risk assessment to determine whether different monitoring approaches are appropriate for

all of the provider types in the IRS's Authorized e-file Provider program. If changes are needed, IRS should make appropriate revisions to the monitoring program, internal guidance, job aids, and staff training, as necessary.

Comment

We disagree with this recommendation. Absent requisite statutory authority and funding, changes in the monitoring program, internal guidance, job aids, and staff training will not have value to the overall program performance.

Recommendation 7

The Commissioner of Internal Revenue should standardize the incident reporting requirements for all types Authorized e-file Providers.

Comment

We agree with this recommendation.

Recommendation 8

The Commissioner of Internal Revenue should document intake, storage, and sharing of the security incident data across IRS offices.

Comment

We agree with this recommendation.

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 FraudNet:

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, (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, (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, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548