United States Government Accountability Office

Report to Congressional Requesters

August 2023

SECURITY OF TAXPAYER INFORMATION

IRS Needs to Address Critical Safeguard Weaknesses

Accessible Version

GAO-23-105395

GAO Highlights

Highlights of GAO-23-105395, a report to congressional requesters

August 2023

SECURITY OF TAXPAYER INFORMATION

IRS NEEDS TO ADDRESS CRITICAL SAFEGUARD WEAKNESSES

Why GAO Did This Study

The U.S. tax system is based largely on voluntary compliance. One factor that may influence taxpayers' willingness to voluntarily comply is the confidence that IRS is protecting their personal and financial information.

GAO was asked to review IRS's safeguards for taxpayer information. This report evaluates the extent to which IRS is following its tax safeguards for protecting taxpayer information.

To address this objective, GAO analyzed mandatory training and UNAX data for IRS employees and contractors, reviewed IRS and TIGTA documentation, and interviewed IRS and TIGTA officials at selected offices. In addition, GAO reviewed federal law authorizing other federal agencies to receive taxpayer information.

GAO also identified and tested selected management, operational, and technical controls on selected IRS systems that store or process taxpayer information, and observed controls in operation. GAO also has ongoing work assessing IRS's efforts to protect the confidentiality of taxpayer information, including its implementation of technical controls and breach response processes. GAO will publish this work in a subsequent report with limited distribution.

Further, GAO reviewed previously issued reports and recommendations, including those issued by TIGTA. GAO categorized them according to the five core security functions described in the NIST cybersecurity framework.

What GAO Found

The Internal Revenue Service (IRS) has implemented access controls and other safeguards to help mitigate risks to taxpayer information. However, continuing weaknesses pose a risk. Among its safeguards, in July 2022, IRS began requiring certain employees to seek senior executive approvals to gain access to taxpayer information. IRS employees also met the agency-wide 97 percent completion goal for training on protecting taxpayer information. However, IRS did not have a training goal for contractors, who had training completion rates well below employee completion rates—less than 75 percent. For example, 66 percent of the approximately 14,000 contractors assigned the Insider Threat Awareness training completed the course. As a result, IRS contractors are at increased risk of being unprepared to handle taxpayer information.

IRS Contractor and Employee Training Completion Rate, Fiscal Year 2021

	IRS Annual Cybersecurity Awareness Training	Insider Threat Awareness	Privacy, Information Protection & Disclosure	UNAX Awareness
Contractor training	74%	66%	69%	69%
Employee training	≥97%	≥97%	≥97%	≥97%

Source: GAO analysis of Internal Revenue Service (IRS) Integrated Talent Management System data. | GAO-23-105395

Accessible Data for IRS Contractor and Employee Training Completion Rate, Fiscal Year 2021

Category	IRS Annual Cybersecurity Awareness Training	Insider Threat Awareness	Privacy, Information Protection and Disclosure	UNAX Awareness
Contractor training	74 percent	66 percent	69 percent	69 percent
Employee training	greater than or equal to 97 percent	greater than or equal to 97 percent	greater than or equal to 97 percent	greater than or equal to 97 percent

Source: GAO analysis of Internal Revenue Service (IRS) Integrated Talent Management System data. | GAO-23-105395

In certain circumstances, IRS faces challenges ensuring taxpayer information it shares—as authorized by law—is properly protected. Federal tax law gives IRS the authority to inspect safeguards for agencies that receive taxpayer information from IRS in certain circumstances. However, in other cases where IRS shares taxpayer information pursuant to different statutory authority, it does not have direct authority to inspect agency safeguards. For these cases, Congress could provide IRS with direct authority to inspect agencies' safeguards, which would give IRS additional assurance that information will be protected sufficiently.

IRS policy requires the agency to maintain an inventory of its systems that store taxpayer information and to mitigate weaknesses in systems that lead to a higher risk of unauthorized disclosure of federal tax information or UNAX—the willful unauthorized access, attempted access, or inspection of federal tax information. However, as of December 2022, IRS omitted seven tax processing systems from its inventory. This limits its monitoring of UNAX prevention efforts.

GAO found that multiple IRS offices oversee contractors but IRS does not have overall oversight efforts related to IRS contractor UNAX. As a result, IRS has limited insight into contractor UNAX trends and assumes greater risk of missing opportunities to improve the agency's prevention efforts.

Weaknesses in IRS's information security controls present risks to taxpayer information. For example, IRS did not assess the risks of its method for transferring taxpayer information to contractors. Until IRS remediates these weaknesses, it will have limited assurance that taxpayer information is protected appropriately.

What GAO Recommends

Since fiscal year 2010, GAO has made 451 recommendations to IRS aimed at safeguarding taxpayer information. While IRS has implemented many of these recommendations, 77 of them had not been implemented as of March 2023. These include two recommendations that GAO considers high priority. Fully implementing these recommendations could significantly improve IRS's ability to safeguard taxpayer information.

In addition to the remaining recommendations above, GAO is making one matter for congressional consideration. This matter would provide IRS with additional authority to inspect agencies' data safeguards in those instances where IRS shares taxpayer information but does not have direct authority to inspect agency safeguards.

GAO is making 15 additional recommendations. These include IRS

- establishing agency-wide training completion goals for contractors;
- maintaining a comprehensive inventory of systems that store or process taxpayer information;
- monitoring contractor UNAX and unauthorized disclosure cases and trends; and
- assessing risks of its method to transfer taxpayers' data electronically to contractors.

IRS agreed with 14 recommendations and disagreed with one. GAO maintains that this recommendation remains warranted, as discussed in the report.

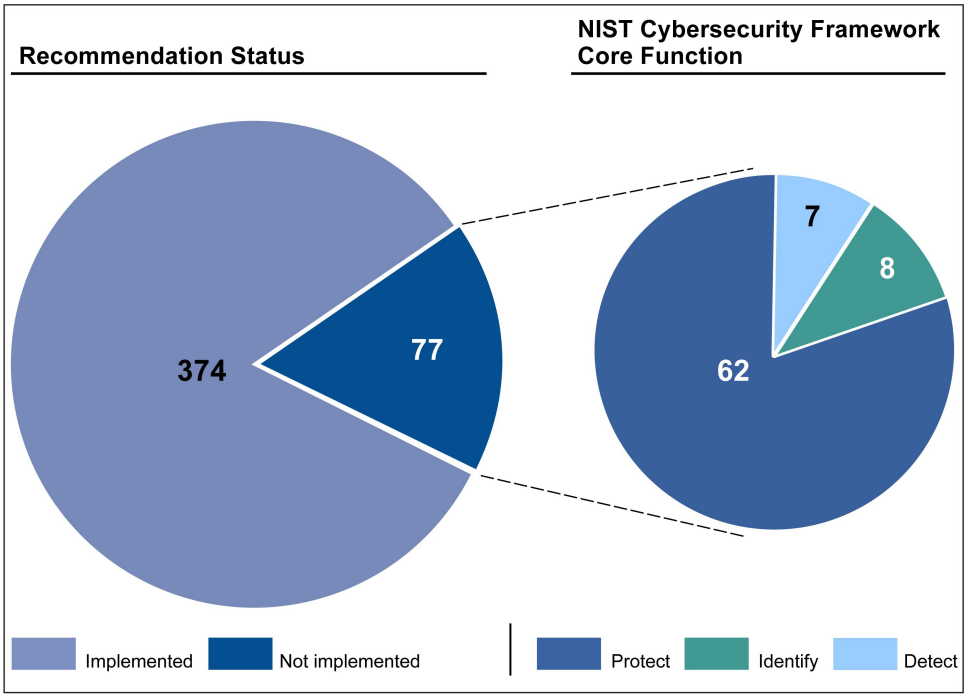
View GAO-23-105395. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov or Jessica Lucas-Judy at (202) 512-6806 or LucasJudyJ@gao.gov.

GAO and the Treasury Inspector General for Tax Administration (TIGTA) have previously reported on deficiencies in IRS's safeguards over taxpayer information. They have both made recommendations aimed at improving these safeguards. Since fiscal year 2010, GAO has made 451 recommendations to strengthen IRS safeguards for taxpayer information in areas such as governance for protecting taxpayer information; authentication and access to tax processing systems; and IRS monitoring of programs that process taxpayer information.

GAO's recommendations cover the five National Institute of Standards and Technology (NIST) cybersecurity core functions that provide a strategic view of life cycle management of cybersecurity risk. A majority of the recommendations cover the *protect* core function (74 percent)—actions related to developing and implementing appropriate safeguards. The remaining recommendations are in the other core functions—*identify*, *detect*, *recover*, and *respond*.

IRS had implemented 83 percent of GAO recommendations as of March 2023.

Status of GAO Recommendations Related to Protecting Taxpayer Information and NIST Cybersecurity Core Function, Fiscal Years 2010–March 2023



Sources: GAO analysis of National Institute of Standards and Technology (NIST) Cybersecurity Framework and GAO recommendations to the Internal Revenue Service. | GAO-23-105395

Accessible Data for Status of GAO Recommendations Related to Protecting Taxpayer Information and NIST Cybersecurity Core Function, Fiscal Years 2010–March 2023 (one of two)

Status	Percentage
Implemented	374
Not Implemented	77

Sources: GAO analysis of National Institute of Standards and Technology (NIST) Cybersecurity Framework and GAO recommendations to the Internal Revenue Service. | GAO-23-105395

Accessible Data for Status of GAO Recommendations Related to Protecting Taxpayer Information and NIST Cybersecurity Core Function, Fiscal Years 2010–March 2023 (two of two)

Status	Percentage
Protect	62
Identify	8
Detect	7

Sources: GAO analysis of National Institute of Standards and Technology (NIST) Cybersecurity Framework and GAO recommendations to the Internal Revenue Service. | GAO-23-105395

Since fiscal year 2019, TIGTA has made 246 recommendations to IRS related to protecting taxpayer information. As of April 2023, according to IRS, it has taken steps to address 202 of them—including implementing controls to manage IT supply chain risks—reducing the risk for disruptions to IRS's operations.

While IRS has taken substantial action to implement GAO recommendations, IRS did not always do so timely. For example, five recommendations have been open for more than 7 years. Additionally, IRS has yet to implement two recommendations GAO identified as high priority—updating a system modernization plan to more fully assess risk and developing a guidance structure to better protect taxpayer information while at third-party providers. Addressing the remaining GAO recommendations could help IRS better manage system security risks, implement safeguards to ensure protected service delivery, and identify cybersecurity events and incidents.

Contents

Tables

Figures

Abbreviations

CDW	Compliance Data Warehouse
COR	contracting officer representative
COVID-19	Coronavirus Disease 2019
FISMA	Federal Information Security Modernization Act of 2014
IRS	Internal Revenue Service
IT	information technology
LB&I	Large Business and International Division
NIST	National Institute of Standards and Technology
PGLD	Privacy, Governmental Liaison and Disclosure
RAAS	Office of Research, Applied Analytics, and Statistics
SB/SE	Small Business/Self-Employed Division
TIGTA	Treasury Inspector General for Tax Administration
UNAX	willful unauthorized access, attempted access, or inspection of federal tax information
W&I	Wage & Investment Division
YK1	Link Analysis Tool

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

August 14, 2023

The Honorable Mike Crapo
Ranking Member
Committee on Finance
United States Senate

The Honorable Jason Smith
Chairman
Committee on Ways and Means
House of Representatives

The Internal Revenue Service (IRS) receives a great deal of personal and financial information about individuals and businesses as part of those taxpayers meeting their tax and filing obligations. While taxpayers face criminal and civil penalties if they do not provide this information, our tax system is based largely on voluntary compliance. To support the goal of voluntary compliance, taxpayers must have confidence that IRS properly protects their personal and financial information.

IRS relies extensively on IT to carry out its mission of providing service to America's taxpayers in meeting their tax obligations. In 2022, IRS collected about $4 trillion in taxes, processed approximately 260 million tax returns, and issued more than $600 billion in refunds and outlays. IRS also relies on IT to process the 4 billion information returns (e.g., the Form 1099 series and Form W-2) it processes annually to verify information taxpayers report on their returns. IT systems support IRS's mission-related operations and information security controls are to protect the confidentiality of the sensitive taxpayer information that resides on those systems.

We first designated information security as a government-wide high-risk area in 1997.[1] In September 2018 and again in March 2021, our high-risk reports emphasized the need for the federal government to take actions to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight,

[1]GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: Feb. 1, 1997), and *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: Feb. 1, 1997).

(2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[2] Most recently, we continued to identify federal information security as a government-wide high-risk area in our April 2023 high-risk update.[3]

We and the Treasury Inspector General for Tax Administration (TIGTA) have reported deficiencies in IRS's safeguards of taxpayer information. In November 2022, we reported that IRS had continuing information system security control deficiencies in such areas as encryption and configuration of security settings that increase the risk of unauthorized access to, modification of, or disclosure of sensitive taxpayer data.[4] In October 2022 in its most recent annual major management and performance challenge report, TIGTA identified protecting taxpayer data as a top challenge for IRS.[5]

Additionally, recent events have raised similar concerns. In August 2022, IRS discovered that it had inadvertently disclosed some taxpayer information that was to be kept confidential on its website. In December 2022, IRS was informed that some of the data appeared to have been disclosed again and discovered that the majority of those data had been inadvertently disclosed on its website.[6] Further, a news organization reported it obtained a large amount of IRS tax data on certain types of taxpayers and published articles based on that information.[7]

[2]See GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021), and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[3]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[4]GAO, *Financial Audit: IRS's FY 2022 and FY 2021 Financial Statements*, GAO-23-105564 (Washington, D.C.: Nov. 10, 2022).

[5]Treasury Inspector General for Tax Administration, *Major Management and Performance Challenges Facing the IRS for Fiscal Year 2023* (Washington, D.C.: Oct. 22, 2022).

[6]We have ongoing work related to these disclosure incidents and will publish this work in a subsequent report with limited distribution.

[7]ProPublica, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax* (June 8, 2021).

You asked us to review IRS's policies and procedures for protecting taxpayer information. In May 2022, we reported on the characteristics of cases of willful unauthorized access and disclosure of taxpayer information by IRS employees for fiscal years 2012 through 2021.[8] This report evaluates the extent to which IRS is following its tax safeguards for protecting taxpayer information.

To address this objective, we analyzed TIGTA's and our prior reports and recommendations related to cybersecurity and protecting taxpayer information. We also analyzed IRS's actions to implement these recommendations. We identified the implementation status of TIGTA recommendations on TIGTA's website (https://www.tigta.gov/reports/list). According to a TIGTA official, recommendations are closed when planned corrective actions are taken. The official also stated that TIGTA neither validates the recommendation statuses nor requires validation before IRS closes recommendations. We did not assess the validity of the recommendation status information identified on TIGTA's website.

We reviewed our prior work related to protecting taxpayer information. We have performed a large body of work related to aspects of cybersecurity at IRS. For example, we annually audit IRS's financial statements to determine whether (1) the financial statements are fairly presented, and (2) IRS management maintained effective internal control over financial reporting. This audit focuses on key systems relevant for storing, processing, and transmitting taxpayer and administrative financial information. It also generally includes recommendations related to cybersecurity protections. We have also reviewed other aspects of cybersecurity at IRS, including the agency's response to breaches of personally identifiable information, the performance of IRS IT investments and risks of IRS legacy systems, taxpayer authentication, and IRS

[8]GAO, *IRS Security of Taxpayer Information: Characteristics of Employee Unauthorized Access and Disclosure Cases*, GAO-22-105872 (Washington, D.C.: May 19, 2022). We also have ongoing work assessing the extent to which IRS appropriately designed and implemented technical controls to protect the confidentiality of federal tax information. We will publish this work in a subsequent report with limited distribution.

oversight of third-party cybersecurity practices.[9] For reporting purposes, we categorized the security controls that we assessed into the five core security functions described in the National Institute of Standards and Technology (NIST) cybersecurity framework.[10]

- **Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[11]
- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

We also analyzed IRS documentation (e.g., procedures, guidance), IRS data, and relevant laws (e.g., Taxpayer Browsing Protection Act of 1997 and Internal Revenue Code section 6103); tested selected management, operational, and technical controls (e.g., safeguards prescribed for a system to protect the confidentiality of the system and its information); reviewed our and TIGTA's prior reports; and interviewed knowledgeable IRS and TIGTA officials.

[9]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34 (Washington, D.C.: Dec. 9, 2013); *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018); *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts,* GAO-18-418 (Washington, D.C.: June 22, 2018); and *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices,* GAO-19-340 (Washington, D.C.: May 9, 2019).

[10]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

[11]According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an affect on organizational operations (including mission, capabilities, or reputation). National Institute of Standards and Technology, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Volume 2, Revision 1 (Gaithersburg, MD: December 2021), 62.

As part of this work, we selected five IRS offices to understand how they protect taxpayer information and the challenges they face in doing so.[12] Specifically, we selected:

- Criminal Investigation;
- Large Business and International Division's Pass-Through Entities office;
- Office of Research, Applied Analytics, and Statistics;
- Small Business/Self-Employed Division's Collection office; and the
- Wage & Investment Division's Accounts Management office.

We selected these offices to ensure they would reflect different types of activities and variation in the amount of willful unauthorized access, attempted access, or inspection of tax returns or return information (UNAX) violations. This selection provided us with a more comprehensive understanding of the different uses and safeguards of taxpayer information.

We analyzed fiscal year 2021 data on completion rates of mandatory training courses related to protecting taxpayer information from the Department of the Treasury's Integrated Talent Management system for IRS employees and contractors. We reviewed related documentation, interviewed knowledgeable IRS officials, and conducted electronic data testing. We determined the Integrated Talent Management System data to be sufficiently reliable for our purposes of reporting training completion rates for fiscal year 2021.

We analyzed fiscal year 2017 through 2021 data from IRS's e-Trak Report of Investigation Unit system on UNAX and unauthorized disclosure cases and related documentation. We interviewed officials to determine how IRS monitors contractor UNAX and unauthorized disclosure cases. To assess the reliability of the data, we compared the data to similar data sources and conducted electronic testing. We also

[12]Our work based on these selected offices is nongeneralizable but gives us broad coverage to the different types of activities in which IRS engages—customer service, collecting taxes owed, complex tax returns and issues, examination, research and data management, and law enforcement. For more information on how we selected these offices, see appendix I.

reviewed IRS documentation and interviewed IRS officials. We found limitations with the data that we discuss in the report.

We also evaluated the controls for five selected IRS systems that process taxpayer information.[13] To select these systems, we identified systems our selected IRS offices accessed and excluded those that we had tested within the past 3 years as part of our annual audit of IRS's financial statements.

We compared the information we collected to various criteria including (1) federal guidance (e.g., NIST guidance); (2) federal internal control standards related to documentation, quality information, and monitoring; (3) IRS plans, policies, and procedures (e.g., the *Internal Revenue Manual*); and (4) our guide for designing evaluations.[14]

For a more detailed description of our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from August 2021 to August 2023 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.

[13]Because we focused our evaluation on five systems, the results of our review of information security controls cannot be generalized to the entire IRS environment.

[14]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020); GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014); Internal Revenue Service, *Internal Revenue Manual* § 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements (July 10, 2018); and GAO, *Designing Evaluations: 2012 Revision (Supersedes PEMD-10.1.4)*, GAO-12-208G (Washington, D.C.: Jan. 31, 2012). See appendix I for details on the specific documentation and criteria we used.

Background

Components of Taxpayer Information

Federal tax information, which we refer to in this report as taxpayer information, consists of federal tax returns and return information (any information derived from a return) that IRS possesses or controls and is covered by the confidentiality safeguards of the Internal Revenue Code.[15] Taxpayer information includes information received directly by IRS or obtained through an authorized secondary source such as the Social Security Administration or another entity acting on IRS's behalf.

- **Returns**. A return is any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the Internal Revenue Code and filed with IRS by, on behalf of, or with respect to any person or entity. Information returns are forms filed by third parties (e.g., employers and financial institutions) that provide information about taxable transactions and submitted to IRS, the Social Security Administration, and taxpayers.
- **Return information**. Return information, in general, is any information collected or generated by IRS regarding any taxpayer's tax liability or possible liability.[16] For example, return information includes the status of a return (whether it is under audit) and data extracted from a return, such as the names of dependents, and the location of a business.

In certain circumstances, IRS is permitted to disclose taxpayer information to other entities, such as federal, state, and local agencies.[17] For example, IRS shares taxpayer information with state tax agencies to improve tax administration.[18] As a condition of receiving this information,

[15]26 U.S.C. § 6103(b)(1), (3).

[16]Return information also includes certain agreements and related information entered into by IRS and the taxpayer. 26 U.S.C. § 6103(b)(2).

[17]See e.g., 26 U.S.C. § 6103(d), (h), (i), (*l*).

[18]See 26 U.S.C. § 6103(d).

the receiving agency must demonstrate, to the satisfaction of IRS, the ability to protect the information's confidentiality.

IRS also may disclose taxpayer information to nongovernmental entities, such as contractors. In these instances, IRS requires that contractors protect this information. IRS contracts are to contain standard language with privacy protections. In these instances, the shared information is still considered taxpayer information and protected from further disclosure.

How IRS Uses Taxpayer Information

To carry out its responsibilities of collecting taxes, processing returns, and enforcing tax laws, IRS uses taxpayer information for many different purposes, as shown in table 1. IRS also enters into agreements or contracts with outside entities for certain services. In selected instances, the entities may be granted access to taxpayer information.[19]

Table 1: Selected IRS Offices' Use of Taxpayer Information

Selected Office	Uses of Taxpayer Information	Contractors' Use of Taxpayer Information
Criminal Investigation	To build criminal cases and provide evidence for prosecution.	To build criminal cases and provide evidence for prosecution.
Large Business & International Division, Pass-Through Entities	For many purposes, including to examine returns and identify areas of high-compliance risk among large, complex businesses and high-wealth taxpayers.	To help find solutions to challenges the organization faces with compliance programs (e.g., how to identify a population of taxpayers).
Office of Research, Applied Analytics, and Statistics	To conduct research, produce statistics, and support tax policy and budget formulation.	For multiple purposes, including to support data analysis or modeling related to compliance projects and so that outside researchers to conduct tax research designed to improve tax administration or the understanding of the tax system's effects.
Small Business/Self-Employed Division, Collection	For many purposes, including to enforce filing and payment requirements and collect payments on unpaid accounts.	To collect overdue tax bills and provides these agencies with taxpayer information (e.g., taxpayer name, Taxpayer Identification Number, balance due, taxpayer contact information) via secure data transfer.
Wage & Investment Division, Accounts Management	To assist taxpayers, including to answer phone calls and correspondence.	Not applicable. This office does not work with contractors that access taxpayer information.

Source: Internal Revenue Service (IRS) information. | GAO-23-105395

[19]For purposes of our report we use the term "IRS contractor" to refer to all individuals and organizations with contractual arrangements with IRS, including consultants, contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers, who may have access to taxpayer information. For our report we focused on contractors with access to taxpayer information.

Note: We selected five IRS offices to understand how they protect taxpayer information and the challenges they face in doing so. We selected offices to ensure they would have varying characteristics, such as different types of work and variation in the amount of relevant violations.

IRS staff—employees and contractors—are responsible for accessing taxpayer information only when it is required to complete official IRS duties as assigned. They are also responsible for protecting the confidentiality and privacy of taxpayer information to which they have access.

If IRS staff access taxpayer information that is not a part of their assigned duties, or is otherwise prohibited, then this access is unauthorized.[20] Unauthorized access can either be considered inadvertent or willful. One type of inadvertent access can occur when IRS staff accidentally accesses tax account information incorrectly by entering an incorrect Taxpayer Identification Number (e.g., Social Security number) in IRS IT systems. The willful unauthorized access, attempted access, or inspection of tax returns or return information is referred to as "UNAX."

IRS staff are only permitted to disclose taxpayer information if there is a statutory basis that allows the disclosure, the proper authorization to disclose this information has been granted, and written procedures for making the disclosure exist.[21] When deciding to disclose taxpayer information, IRS staff are to consider a number of factors, including the authentication of the intended recipient and the recipient's need to know.

Similar to unauthorized access, unauthorized disclosures of taxpayer information can be considered inadvertent or willful. Inadvertent disclosures are unintended, whereas willful unauthorized disclosures, or what for the rest of this report we are referring to as unauthorized disclosure, are intentional.

[20]IRS guidance outlines specific relationships and criteria by which IRS staff are not authorized under any circumstances to access taxpayer information. Examples include accessing information regarding an employee's or contractor's spouse, children, and other relatives; or those they may have a personal or outside business relationship. IRS staff are also prohibited from accessing celebrities'—a person who is famous, widely known, or frequently in the media—and politicians' taxpayer information unless they have a legitimate tax-related reason to access them. Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.5(2) Employee UNAX Responsibilities (Mar. 8, 2023) and *Internal Revenue Manual* § 10.5.5.5(1) Covered Relationships (Mar. 8, 2023).

[21]Internal Revenue Service, *Internal Revenue Manual* § 11.3.1.2(2) Disclosure Code, Authority and Procedure (CAP) (Mar. 13, 2018).

In May 2022 we reported that of the UNAX cases IRS could substantiate, about 82 percent resulted in the offending employee's suspension, resignation, or removal. Similarly, for the cases where IRS found employees committed both UNAX and unauthorized disclosure violations, all cases resulted in the offending employee's suspension, resignation, or removal.[22]

Safeguards for Taxpayer Information

Laws and Guidance Providing Safeguards for Taxpayer Information

Substantially amended in 1976, section 6103 of the Internal Revenue Code provides confidentiality protections and safeguards for taxpayer information.[23] Prior to passage of the section 6103 amendments in the Tax Reform Act in 1976, the executive branch had discretion over decisions to share taxpayer information. By the mid-1970s, Congress and the public were growing more concerned about government agencies using tax information for purposes unrelated to tax administration. The 1976 amendments to section 6103 were written to address concerns about the potential for too much dissemination of tax information and the misuse of tax information.

Nevertheless, concerns remained about IRS's ability to prevent and detect UNAX that had occurred. For example, in April 1997, we reported on continuing shortcomings in IRS's efforts to prevent unauthorized access to confidential taxpayer data.[24] We noted that IRS did not (1) monitor all employees with access to automated systems and data for evidence of unauthorized access, (2) consistently investigate cases

[22]For more information on the characteristics of IRS employee UNAX and unauthorized disclosure cases, see GAO-22-105872.

[23]26 U.S.C. § 6103. These confidentiality safeguards continue to apply when IRS shares taxpayer information with other entities, such as other federal or state agencies, pursuant to section 6103.

[24]GAO, *IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses*, GAO/AIMD-97-49 (Washington, D.C.: Apr. 8, 1997).

involving unauthorized access, and (3) consistently discipline employees who accessed taxpayer data without authorization.

As a result of these concerns, Congress passed and the President signed the Taxpayer Browsing Protection Act of 1997, which made the willful unauthorized inspection of taxpayer returns or return information by staff a crime.[25] The willful unauthorized disclosure of a taxpayer's return or return information is also a crime.[26]

Federal laws—including the Federal Information Security Modernization Act of 2014 (FISMA)—and guidance specify requirements for protecting the security and privacy of federal information and systems, including those that IRS uses to process and store taxpayer information.[27]

- **FISMA**. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over federal operations and assets.[28] FISMA assigns responsibility to each agency head for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The law also delegates the authority to ensure compliance with FISMA requirements to the agency chief information officer (or comparable official). This officer is responsible for designating a senior agency information security officer whose primary duty is information security.

[25]Pub. L. No. 105-35, § 2, 111 Stat. 1104, 1104–1105 (1997), *codified at* 26 U.S.C. § 7213A. The act also requires notification of and authorizes civil damages for unlawful access or disclosure. Pub. L. No. 105-35, § 3, 111 Stat. at 1105–1106, *codified at* 26 U.S.C. § 7431. Instead of "browsing," IRS uses the acronym "UNAX" to cover all cases of willful unauthorized access or inspection of taxpayer records. We use UNAX in our report.

[26]26 U.S.C. § 7213.

[27]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), Title III of Pub. L. No. 107-347. As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect. This act provides a comprehensive framework for ensuring the effectiveness of information security controls over federal agency operations and assets.

[28]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (2014), *codified at* 44 U.S.C. § 3551.

The law also requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based safeguards for the information and information systems that support the operations and assets of the agency. Such a program includes (1) assessing risks; (2) developing and implementing policies and procedures to cost effectively reduce risks; (3) developing and implementing plans for providing adequate information security for networks, facilities, and systems; (4) providing security awareness training; (5) testing and evaluating the effectiveness of controls; (6) planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; (7) developing and implementing procedures for detecting, reporting, and responding to security incidents; and (8) ensuring continuity of operations.

- **NIST standards**. FISMA and the Office of Management and Budget also require agencies to comply with NIST standards, including minimum information security requirements as described in NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[29] This publication provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets.[30] The publication also provides baseline security controls for low-, moderate-, and high-impact systems. Agencies can then tailor or supplement their security requirements and policies based on agency mission, business requirements, and operating environment.
- **NIST cybersecurity framework**. In May 2017, the President issued an executive order[31] requiring agencies to immediately begin using NIST's cybersecurity framework for managing their cybersecurity

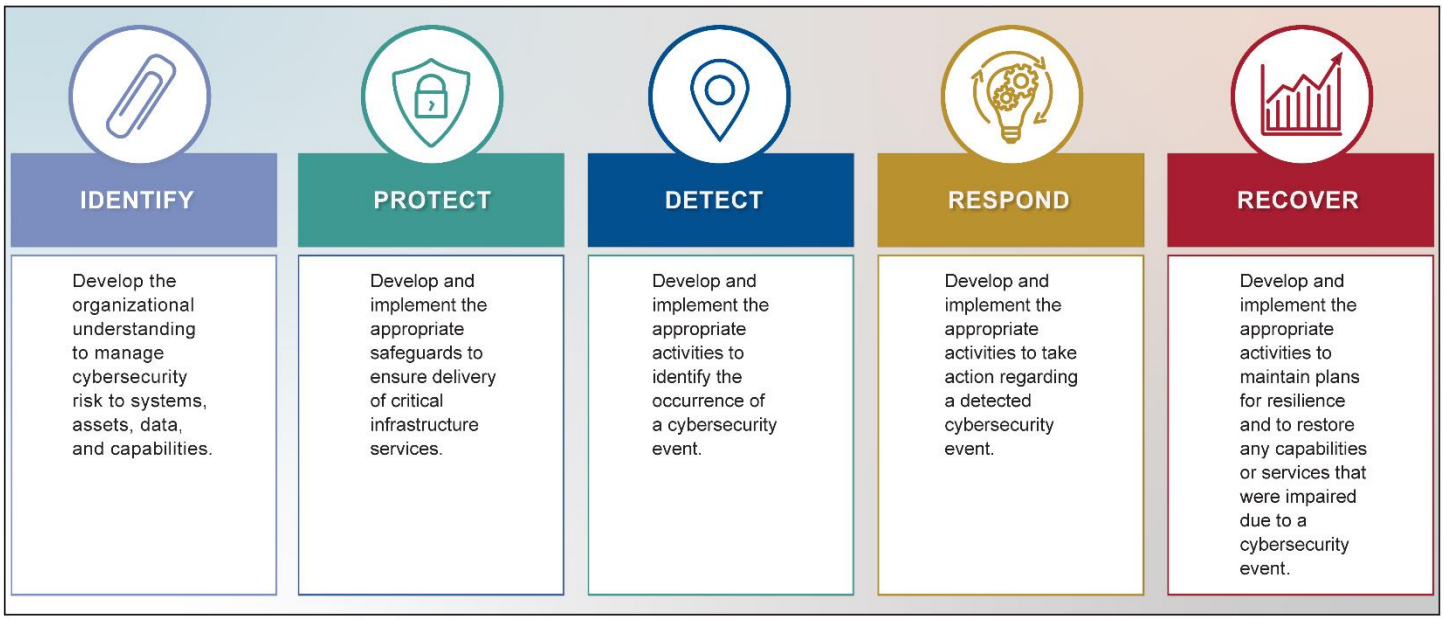
[29]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[30]Security control topics, referred to as families of security controls, covered by NIST Special Publication 800-53 include access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

[31]Exec. Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22391 (May 16, 2017).

risks.[32] As shown in figure 1, the framework, which provides guidance for cybersecurity activities, is based on five core security functions.

Figure 1: National Institute of Standards and Technology Cybersecurity Framework



Sources: GAO presentation of National Institute of Standards and Technology Cybersecurity Framework; bsd studio/stock.adobe.com. | GAO-23-105395

Accessible Data for Figure 1: National Institute of Standards and Technology Cybersecurity Framework

- Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

[32]National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018). The framework was developed in response to an executive order issued by a prior administration (The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013)). It was originally intended for use in protection of critical infrastructure. NIST initially issued guidance in February 2014 and has since revised the framework. NIST is updating the framework and plans to release it in early 2024.

- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Sources: GAO presentation of National Institute of Standards and Technology Cybersecurity Framework; bsd studio/stock.adobe.com. | GAO-23-105395

According to NIST, these five functions occur concurrently and continuously, and provide a strategic view of the life cycle of an organization's management of cybersecurity risk.

Federal law and guidance also require IRS to protect taxpayer information by disposing of it appropriately when no longer needed.

- **Federal Records Act**. Under the Federal Records Act of 1950, IRS is required to maintain an active, continuing program for the economical and efficient management of the records of the agency.[33] The program should provide for effective controls over the creation, maintenance, and use of records in the conduct of current business, including case files. This act also designates the National Archives and Records Administration as responsible for issuing records management guidance and approving the schedule for disposition (destruction or preservation) of records.[34]
- **Office of Management and Budget guidance**. Office of Management and Budget guidance directs agencies to maintain personally identifiable information, including taxpayer information, in accordance with applied Records Control Schedules approved by the National Archives and Records Administration.[35]
- **IRS guidance**. According to the *Internal Revenue Manual*, IRS is to retain and dispose of taxpayer information as required by law to properly maintain confidentiality and prevent disclosure.[36]

[33]44 U.S.C. § 3102.

[34]44 U.S.C. § 3302.

[35]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016). Records control schedules provide mandatory instructions for the disposition of records when they are no longer required by the agency. They provide legal disposition authority for continued retention and preservation of records of historical value, among other things.

[36]Internal Revenue Service, *Internal Revenue Manual* § 1.15.1.2(1)(e), Records Management as it Relates to Other Programs (Feb. 5, 2021).

IRS Policies, Procedures, and Responsibilities for Protecting Taxpayer Information

IRS publishes its information security policies and guidelines in its *Internal Revenue Manual* and other documents to enable IRS staff to carry out their respective responsibilities, including implementing taxpayer information safeguards and information security controls. IRS details UNAX policies, procedures, and requirements that are to be followed by all IRS organizations in one section of the *Internal Revenue Manual* maintained by IRS's Privacy, Governmental Liaison and Disclosure (PGLD) office.[37] IRS provides guidance on aspects of security to protect IT resources in another section of the *Internal Revenue Manual* maintained by the Office of the Chief Information Officer.[38]

Within IRS, PGLD and IT offices have primary responsibility for developing policies to ensure taxpayer information is properly protected.

- **PGLD**. Led by the Chief Privacy Officer, PGLD is responsible for overseeing IRS privacy and records management policies, coordinating privacy protection guidance and activities, responding to privacy complaints, and promoting data protection awareness throughout IRS.[39] As part of this work, PGLD develops policies, standards, and guidelines related to disclosure of information, including federal tax information. PGLD also creates agency-wide privacy training materials and communications pertaining to privacy requirements.

  PGLD also oversees IRS's UNAX Program, which aims to ensure all IRS staff (1) understand what UNAX is; (2) understand the consequences of accessing or inspecting tax information for other than management-authorized tax administration reasons; and (3) work to prevent UNAX violations. PGLD is also responsible for implementing other measures (e.g., developing and distributing

[37]The *Internal Revenue Manual* is the primary, official compilation of instructions to staff that relate to the administration and operation of IRS. For more information on IRS's comprehensive UNAX policies, procedures, and requirements, see Internal Revenue Service, *Internal Revenue Manual* § 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements (Mar. 8, 2023).

[38]See Internal Revenue Service, *Internal Revenue Manual* § 10.8.1, Information Technology (IT) Security, Policy and Guidance (Dec. 13, 2022).

[39]See Internal Revenue Service, *Internal Revenue Manual* § 1.1.27, Privacy, Governmental Liaison and Disclosure (PGLD) (May 7, 2019).

periodic communications, managing the annual UNAX Awareness briefing certification program, and providing managers guidance related to UNAX) designed to foster voluntary UNAX compliance and identify areas for improvement.

PGLD also oversees IRS's records management program, which is responsible for managing the entire life cycle of records, including creation or receipt, maintenance, disposal (destruction), retirement, or transfer of permanent records to the National Archives and Records Administration. As part of this work, PGLD is to ensure the proper access, preservation, and timely disposition of all records according to records control schedules and applicable federal statutes.

- **IT office**. Led by the chief information officer, IRS's IT office is to deliver IT services and solutions to support tax administration. The office is also responsible for protecting IRS's systems, services, and data, including taxpayer information, from internal and external cyber-related threats.[40] In addition, it also conducts auditing and monitoring activities and provides protection of sensitive but unclassified data, including taxpayer information.[41] This office comprises eight suboffices, including the IT Cybersecurity office, which helps to ensure taxpayer information is protected. As part of this effort, this office is responsible for reviewing and certifying various data security reports. The IT Cybersecurity office also analyzes and partners with management to determine the validity of account-related accesses.

Additionally, all IRS staff is responsible for protecting taxpayer information. For example, IRS senior executives and managers are responsible for monitoring, assigning, or removing employee or contractor access to IRS computing systems as needed based on assigned IRS duties. Senior executives and managers should approve access only when it is required to complete official IRS duties. Also, all IRS staff are to take the annual UNAX Awareness Briefing and complete the associated certification documentation if they did not complete the briefing online.

[40]See Internal Revenue Service, *Internal Revenue Manual* § 1.1.12.1, Mission (July 22, 2022), and *Internal Revenue Manual* § 1.1.12.3, ACIO for Cybersecurity (July 22, 2022).

[41]According to IRS officials, the IT Cybersecurity office provides audit and monitoring capabilities to systems that the IRS IT office maintains.

IRS Implemented Safeguards to Protect Taxpayer Information but Needs to Further Address Weaknesses

Historically, we and TIGTA have found gaps in IRS's safeguards for taxpayer information and have made recommendations to help strengthen them. IRS has implemented safeguards aimed at better protecting taxpayer information, such as restricting access to it. Additionally, the selected offices in our review generally followed IRS's UNAX policies. However, IRS's oversight of contractors accessing taxpayer information and selected IT controls have gaps. Further, IRS does not have direct authority to inspect agencies' safeguards for taxpayer information in certain circumstances.

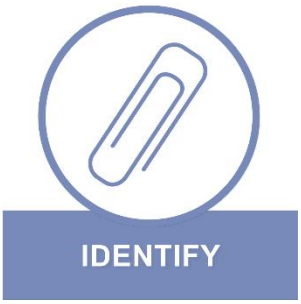
IRS Has Had Substantial Gaps in Protecting Taxpayer Information and Has Implemented 83 Percent of Our Recommendations

Since fiscal year 2010, we have issued 451 recommendations to IRS related to protecting taxpayer information. In addition, we identified 246 recommendations made by TIGTA since fiscal year 2019 to IRS to improve safeguards for taxpayer information. As of March 2023, IRS had taken steps to address the gaps in safeguards we identified and implemented 83 percent of our recommendations. Similarly, IRS reported it had implemented more than 80 percent of TIGTA's recommendations.

Gaps in Safeguards Span Cybersecurity Functions

We have made recommendations to IRS across all five NIST security core functions—*identify*, *protect*, *detect*, *respond*, and *recover*. When considered together, these functions provide a strategic view of the ongoing life cycle of an organization's management of cybersecurity risk.[42]

[42]The distribution of counts of our recommendations across the five core functions does not necessarily correlate with the amount of improvements needed to strengthen IRS safeguards for taxpayer information in each function. The discrepancy in recommendation counts could be due to the objectives and how we designed and scoped our work.



Identify. Since fiscal year 2010, we have made 63 recommendations related to this core security function. Actions related to this function enable an agency to develop an understanding to manage cybersecurity risk to systems, assets, data, supply chain, and capabilities. Of the 63 recommendations, we identified two of our open recommendations as priority recommendations for IRS.[43]

First, in December 2020 we found that IRS's ability to process and use information returns is limited by its outdated legacy IT systems. We recommended that IRS revise the 2017 Information Returns System Modernization plans by evaluating changes in the environment, assessing risks to systems and programs, and detailing how the agency plans to address issues in the intake, processing, and use of information returns across business units.[44]

Although IRS neither agreed nor disagreed with the recommendation, officials reported that IRS will submit an Information Return System Modernization plan to Congress. The officials added that the plan will leverage the 1099 Internet Platform required by section 2102 of the Taxpayer First Act as the foundation of information return modernization efforts.[45] In January 2023, IRS rolled out the release of an internet platform that allows businesses to electronically file IRS Form 1099 information returns for the 2023 filing season. In March 2023, IRS officials also reported that future releases of this platform will modernize the intake and processing of other information return forms, such as those that are currently submitted through IRS's Filing Information Returns Electronically system. Officials noted that future releases of the platform will allow IRS to be more responsive to changes needed for information returns by integrating legislative and other changes in a quicker and more efficient manner.

[43]For more information on these and our other priority recommendations to IRS and their status, see GAO, *Priority Open Recommendations: Internal Revenue Service*, GAO-23-106470 (Washington, D.C.: July 31, 2023).

[44]GAO, *Tax Administration: Better Coordination Could Improve IRS's Use of Third-Party Information Reporting to Help Reduce the Tax Gap,* GAO-21-102 (Washington, D.C.: Dec. 15, 2020).

[45]The act required IRS to develop an internet portal by January 1, 2023, that allows taxpayers to electronically file IRS Forms 1099. Pub. L. No. 116-25, § 2102, 133 Stat. 981, 1010 (2019). According to IRS, this website will provide taxpayers with IRS resources and guidance, and allow them to prepare, file and distribute IRS Forms 1099, and create and maintain tax records.

However, as of March 2023, IRS officials said they are still developing plans related to the specific resources needed, scope, and schedule of the future releases. IRS officials reported that more specific plans were being developed as part of agency planning for the Inflation Reduction Act funding. The April 2023 Inflation Reduction Act Strategic Operating Plan mentions enhancing the information return platform to support digital asset reporting in fiscal year 2023. However, it does not provide more details related to the resources needed, or scope and schedule of the initiative.

Because information returns affect so many areas within IRS, a coordinated approach across the many offices that manage their intake, processing, and use would benefit IRS. For example, coordination would help ensure that the various business units that access the data are able to use the information. A modernized system may also allow for earlier identification and selection of cases for further review. This, in turn, would help IRS to reduce taxpayers' interest payments on misreported income, credits, and deductions.

Second, in May 2019 we found that 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 did not provide assurance that taxpayer information was being adequately protected. We recommended that IRS develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate aspects of IRS's efforts to protect taxpayer information while at third-party providers.[46] IRS agreed with the intent of this recommendation but did not agree to implement it.

To fully implement this recommendation, IRS needs to demonstrate it has a structure to coordinate across seven different offices working on information security-related activities. Actions IRS could take could include updating existing standards, monitoring Authorized e-file Provider program compliance, and tracking security incident reports. Without this structure, it is unclear how IRS will adapt to changing security threats in the future and ensure those threats are mitigated.

[46]GAO, *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices,* GAO-19-340 (Washington, D.C.: May 9, 2019).

In addition, in September 2022, TIGTA recommended that IRS ensure that all recommended countermeasures identified in the most recent risk assessment for each IRS facility are tracked until a new risk assessment is completed using the new countermeasure tracking mechanism.[47] Without tracking the status of countermeasures, IRS lacks assurance that known security vulnerabilities have been mitigated. According to TIGTA's report, IRS plans to address this recommendation by October 2023.

Protect. Since fiscal year 2010, we have made 335 recommendations related to this core security function. Actions related to this function enable an agency to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Our recommendations in this area cover many different topics, including staff knowledge and training; information protection processes and policies; data security; identity management, authentication, and access control; and protective technology. For example, we recommended that IRS fully implement IT workforce planning to include addressing skills gaps.[48] IRS has taken steps to implement this recommendation, including developing plans to operationalize its IT Workforce Strategy. Officials said they intend to implement this recommendation by summer 2023.

In March 2023, TIGTA recommended that IRS ensure that privileged user activity logs—records of an authorized user's activity including accessing a system—are regularly monitored and inactive accounts deactivated in accordance with agency security requirements.[49] The lack of proper monitoring and deactivation of privileged user accounts increases the risk of unauthorized changes to systems.

Additionally, in September 2021, TIGTA recommended that IRS ensure that data at rest be encrypted prior to being transferred from IRS to

[47]Treasury Inspector General for Tax Administration, *The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed*, 2022-10-046 (Washington, D.C.: Sept. 14, 2022).

[48]GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

[49]Treasury Inspector General for Tax Administration, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements,* 2023-20-018 (Washington, D.C.: Mar. 27, 2023).

private collection agencies.[50] Until IRS implements this recommendation, data will remain at risk of exposure or unauthorized access. According to TIGTA's reports, IRS plans to address these recommendations by February 2024 and by August 2023, respectively.

Detect. Since fiscal year 2010, we have made 40 recommendations related to this core security function. Actions related to this function enable an agency to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[51] Our recommendations in this area cover detection processes, anomaly and event detection, and continuous monitoring. For example, we recommended that IRS update monitoring programs for electronic return originators to include techniques to monitor basic information security and cybersecurity issues. Further, IRS should make appropriate revisions to internal guidance, job aids, and staff training, as necessary.[52]

As of February 2023, IRS officials agreed with the intent of the recommendation but did not plan to implement it. IRS reported it does not have the statutory authority to establish policy on information security and cybersecurity issues, nor enforce compliance. However, as we reported IRS already monitors physical aspects of information security, which goes beyond existing Authorized e-file Provider program requirements.[53] We believe that incorporating basic cybersecurity monitoring into the agency's oversight efforts would provide IRS the opportunity to help inform the

[50]Treasury Inspector General for Tax Administration, *The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement,* 2021-20-066 (Washington, D.C.: Sept. 27, 2021). Data at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The encryption of organizational data when at rest ensures that such information is protected and promotes a defense-in-depth security strategy.

[51]According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). National Institute of Standards and Technology, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Volume 2, Revision 1 (Gaithersburg, MD: December 2021), 62.

[52]Electronic return originators originate the electronic submission of tax returns to IRS. They may either prepare returns for clients or collect returns from taxpayers who have prepared their own returns. For more information, see GAO-19-340.

[53]For more information, see GAO-19-340.

most vulnerable third-party providers of additional guidance and resources.

Respond. Since fiscal year 2010, we have made six recommendations related to this core security function. Actions related to this function enable an agency to develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Our recommendations in this area address analyzing cybersecurity incidents to facilitate an effective response, coordinating communications, and applying lessons learned from incidents to improve future response activities. For example, we recommended that IRS require an evaluation of the agency's response to data breaches involving personally identifiable information to identify lessons learned that could be incorporated into agency security and privacy policies and practices.[54] In June 2017, IRS provided evidence to show that it had analyzed trends of incidents. According to its Breach Response Guide, the report will be used to determine if there are any processes for which IRS can perform a risk assessment to identify vulnerabilities and make recommendations to improve the agency's security and privacy policies and practices. As a result, IRS has decreased the risk of experiencing similar data breaches in the future and possibly suffering adverse effects that might have been prevented.

In September 2022, TIGTA recommended that IRS ensure that the User Behavior Analytics Capability team implements a process to document feedback from stakeholders on referred incidents.[55] IRS reported it implemented this recommendation, which can help improve the User Behavior Analytics Capability team's ability to identify potential insider threats.

[54]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

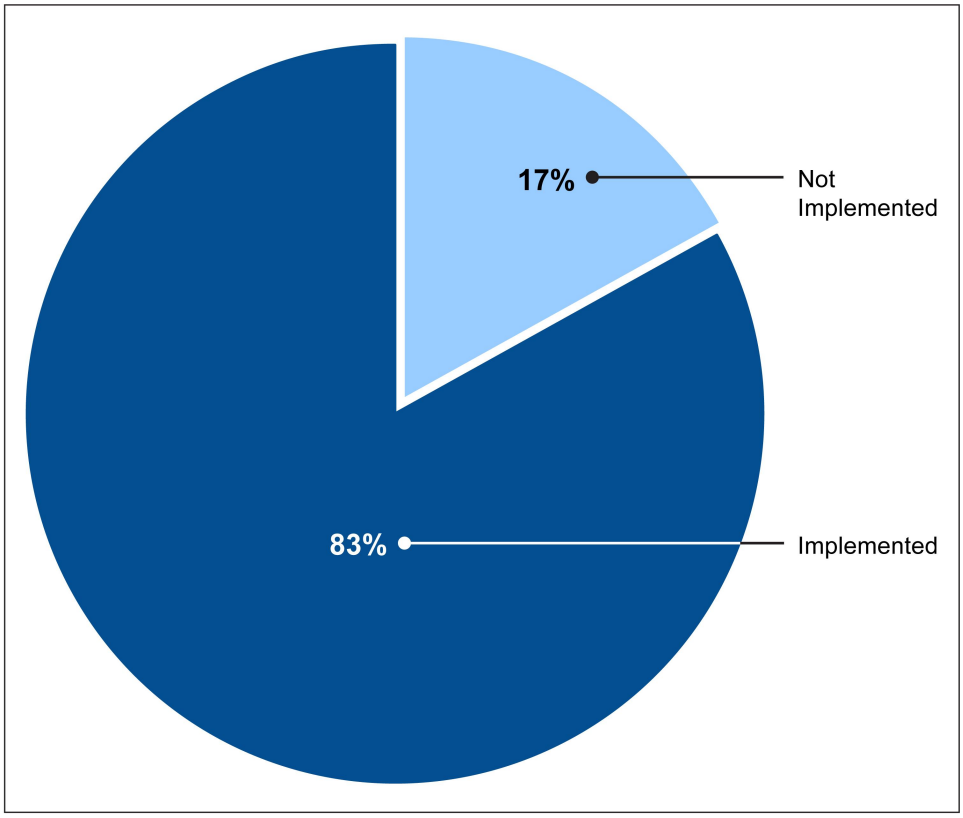
[55]Treasury Inspector General for Tax Administration, *Improvements Are Needed for an Effective User Behavior Analytics Capability,* 2022-20-055 (Washington, D.C.: Sept. 21, 2022).

Recover. Since fiscal year 2010, we have made seven recommendations related to this core security function. Actions related to this function enable an agency to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Our recommendations in this area address recovery planning and lessons learned. IRS has implemented these recommendations, which, for example, has better positioned the agency to recover from disruptions to normal operating conditions and security incidents.

Implementing Remaining Recommendations Would Continue Progress in Protecting Taxpayer Information

As of March 2023, IRS had taken steps to address the gaps in safeguards we identified: of the 451 recommendations we made, IRS had implemented 374 (83 percent) and had not implemented 77 of them (17 percent), as shown in figure 2.

Figure 2: Status of GAO Recommendations Related to Protecting Taxpayer Information, Fiscal Years 2010 – March 2023



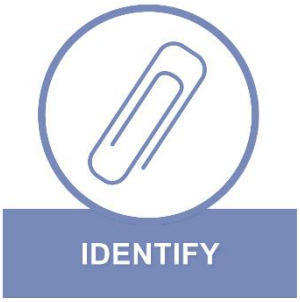
Sources: GAO analysis of GAO recommendations to the Internal Revenue Service. | GAO-23-105395

Accessible Data for Figure 2: Status of GAO Recommendations Related to Protecting Taxpayer Information, Fiscal Years 2010 – March 2023

Status	Recommendations	Percent
Implemented	374	83%
Not Implemented	77	17%

Sources: GAO analysis of GAO recommendations to the Internal Revenue Service. | GAO-23-105395

For example, for the *protect* core function, IRS took action to strengthen taxpayer authentication in response to our recommendations.[56] In February 2020, IRS developed a repeatable, comprehensive process to identify and evaluate alternative options for improving taxpayer authentication. IRS plans to generate ideas to improve authentication through workshops, vendor engagement, use cases, and research. A working group will then research and prioritize ideas and make recommendations to IRS's authentication council. Suggestions approved by the council are then to be provided to the appropriate IRS governance body for approval and delegation. If implemented effectively, this process will help ensure that IRS has a sound rationale for its investment decisions and the resources it needs to make authentication improvements in a timely manner.



As of April 2023, according to IRS, it had taken steps to address 202 of TIGTA's 246 recommendations (82 percent).[57] For example, related to the *identify* core function, in response to TIGTA's recommendation, IRS implemented controls to manage IT supply chain risks. IRS reported it revised the *Internal Revenue Manual* and identified and incorporated other federal agencies' relevant supply chain risk management best practices.[58] By implementing supply chain risk management security controls, IRS will have reduced risk for disruptions to the agency's operations and meet its mission helping taxpayers comply with their tax responsibilities.

As of March 2023, IRS had not implemented 77 of our recommendations to strengthen its safeguards of taxpayer information related to

- developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;

[56]GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts,* GAO-18-418 (Washington, D.C.: June 22, 2018).

[57]TIGTA's website (https://www.tigta.gov/reports/list) displays the statuses of recommendations made to IRS. According to a TIGTA official, the statuses of recommendations are not validated by TIGTA as TIGTA does not require validation before IRS closes recommendations. We did not perform any audit work to validate the recommendation status information that we obtained from TIGTA's website.

[58]Treasury Inspector General for Tax Administration, *More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks,* 2022-20-009 (Washington, D.C.: Feb. 2, 2022).

- developing and implementing the appropriate safeguards to ensure delivery of services; and
- developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event, as shown in table 2.

Table 2: Number of Not Implemented GAO Recommendations Related to Protecting Taxpayer Information by NIST Cybersecurity Framework Core Function, Fiscal Year 2010 – March 2023

NIST Core Security Function	Number of Total Recommendations	Number and Percentage of Not Implemented Recommendation
Identify	63	8 (13 percent)
Protect	335	62 (19 percent)
Detect	40	7 (18 percent)
Respond	6	0 (0 percent)
Recover	7	0 (0 percent)
Total	**451**	**77 (17 percent)**

Source: GAO analysis of National Institute of Standards and Technology (NIST) cybersecurity framework and GAO recommendations. | GAO-23-105395

Note: The distribution of counts of our recommendations across the five core functions does not necessarily correlate with the amount of improvements needed to strengthen IRS safeguards for taxpayer information in each function. The discrepancy in recommendation counts could be due to the objectives and how we designed and scoped our work.

In some instances, IRS has not taken timely action to address our recommendations. For example, of recommendations we made prior to fiscal year 2018, 17 remained open as of March 2023. Five of these have been open more than 7 years. This includes one recommendation that IRS establish procedures to monitor whether non-IRS contractors with unescorted access to IRS facilities are receiving unauthorized access awareness training.[59] During fiscal year 2021, IRS developed a standard operating procedure to establish policies and procedures for monitoring and enforcing training requirements that allow contractors to maintain unescorted access to IRS facilities. As of September 2022, IRS officials told us that they will address this recommendation in the future.

Implementing our outstanding recommendations related to protecting taxpayer information could help IRS better develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities; develop and implement the appropriate safeguards to ensure

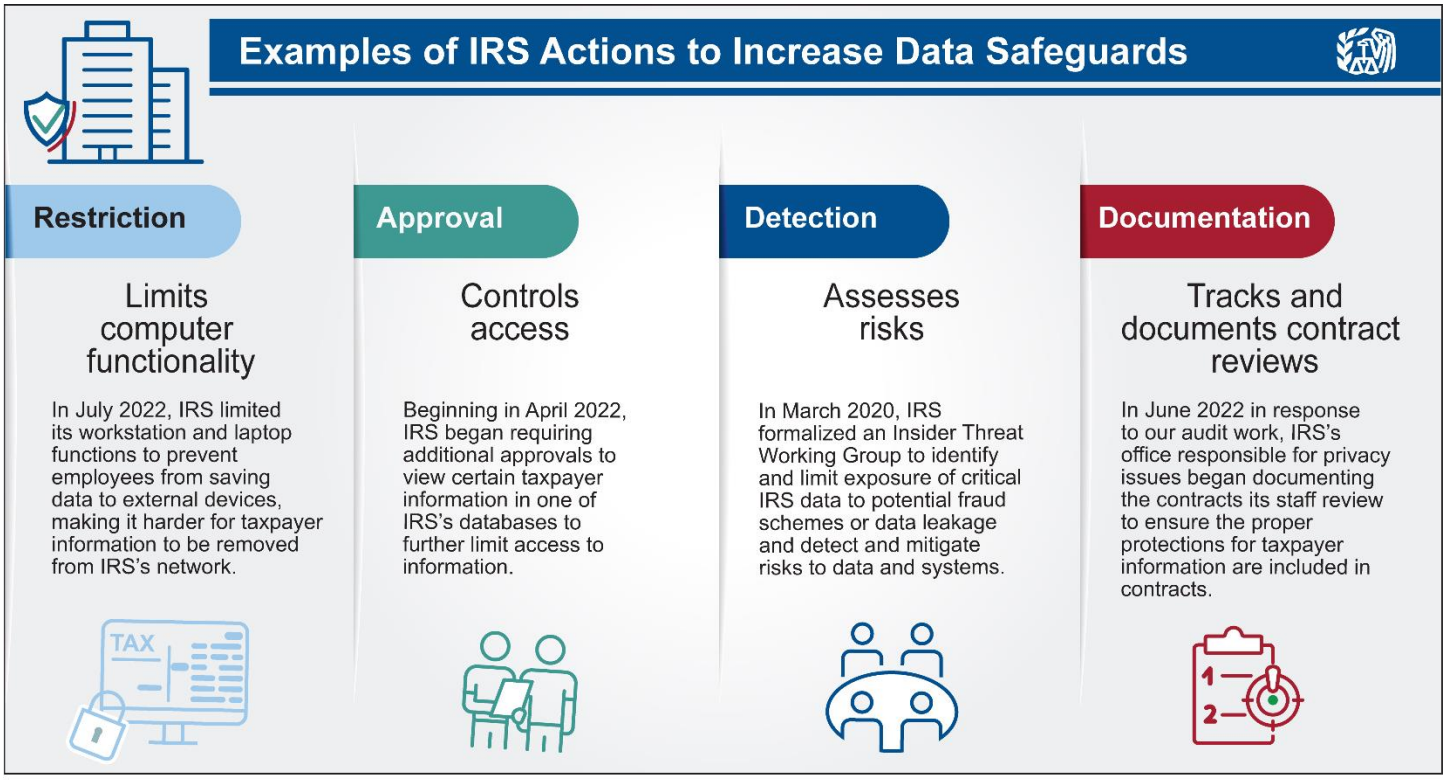
[59]GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting,* GAO-15-480R (Washington, D.C.: May 29, 2015).

delivery of services; and develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Selected Safeguards Restrict Access to Taxpayer Information

IRS has implemented new safeguards to better protect taxpayer information. For example, in July 2022, IRS began requiring its staff to re-establish their access to taxpayer information in certain IT systems and have Senior Executive Service approval for this access. IRS's new safeguards relate to restricting access to taxpayer information, requiring approval to see this information, detecting risks, and documenting contract reviews (see fig. 3).

Figure 3: Examples of IRS Actions to Increase Data Safeguards



Sources: GAO analysis of Internal Revenue Service (IRS) information; bsd studio/stock.adobe.com and FourLeafLover/stock.adobe.com. | GAO-23-105395

In April 2022, IRS began requiring additional approvals to access taxpayer data that contained personally identifiable information (e.g., name and Taxpayer Identification Number) in one of its databases. According to officials, this change is intended to mitigate risks and limit the access to personally identifiable information, without affecting the demand for taxpayer data to use for research. IRS masked personally identifiable information in some of its datasets. According to officials, this change enables users to conduct tax research without viewing sensitive information.

However, in some cases it is necessary for researchers to view personally identifiable information for their work. For additional protection, this information is segregated by type (e.g., individual files, business filers) and access to it requires additional approvals and justification. According to IRS officials, this segregation limits the amount of taxpayer information users could access. For example, according to IRS documentation, personally identifiable information can provide important contextual information for research, such as names and addresses helping researchers understand if people are related or live together.

IRS has taken steps to respond to a news organization's claim that it had acquired taxpayer information. For example, officials in one of our selected offices said they reviewed their data systems to ensure there had not been any UNAX incidents in response to this reporting.

IRS officials also said they have taken steps to address challenges related to monitoring UNAX incidents. They said it is challenging to identify all UNAX and unauthorized disclosure incidents because managers cannot monitor all of their staff all of the time. Officials further explained that depending on the nature of the work, it can be hard to identify suspicious accesses. For example, it can be difficult to identify suspicious accesses when staff are accessing large amounts of data to do research.

IRS officials said they mitigate the risks of not being able to continuously monitor all staff by ensuring staff accessing taxpayer information have background investigations, receive training, and are aware of the consequences of UNAX and unauthorized disclosure of taxpayer information. For example, IRS conducts background investigations for its staff prior to giving them access to taxpayer information, which can include checking credit and fingerprinting. IRS implemented IT controls to identify instances when its staff access taxpayer information without

authorization on some, but not all, IRS systems that process taxpayer information, as will be discussed later in this report.

Selected Offices Generally Follow UNAX Policies

Officials in our selected offices were generally aware of agency-wide policies to protect taxpayer information. However, as discussed above, we previously reported that IRS had continuing information system security control deficiencies that increase the risk of unauthorized access to or disclosure of taxpayer information.[60] Additionally, in this review we found that IRS contractors had low training completion rates for courses related to protecting taxpayer information, creating a risk that they may not know how to properly protect taxpayer information. Further, if contractors commit UNAX or unauthorized disclosure, some IRS officials responsible for overseeing contractors did not know how to report those incidents, potentially constraining IRS's ability to provide appropriate and timely incident responses.

Selected Offices Generally Follow Agency-wide UNAX Policies for Protecting Taxpayer Information

Based on our analysis of IRS data, the selected offices had a low amount of substantiated UNAX cases from fiscal years 2012 through 2021. The offices ranged from having no substantiated UNAX cases to having 161 substantiated UNAX cases over the 10-year period. The office with the highest amount of cases averaged about 16 UNAX cases per year during this time period.[61]

[60]We reviewed the results of our recent audits of IRS's financial statements, including our subsequently issued management reports presenting new deficiencies in IRS's internal control over financial reporting and the status of IRS's corrective actions to address prior deficiencies. GAO, *Financial Audit: IRS's FY 2022 and FY 2021 Financial Statements*, GAO-23-105564 (Washington, D.C.: Nov. 10, 2022); *Management Report: IRS Needs to Improve Financial Reporting and Information System Controls*, GAO-22-105559 and GAO-22-105558SU (Limited Official Use Only version) (Washington, D.C.: May 25, 2022); and *Financial Audit: IRS's FY 2021 and FY 2020 Financial Statements*, GAO-22-104649 (Washington, D.C.: Nov. 10, 2021).

[61]According to IRS officials, this office has about 20,000 employees and all of its work involves accessing taxpayer information. As discussed below, different IRS offices have different amounts of staff accessing taxpayer information.

According to IRS's *Internal Controls Managerial Assessment* for fiscal year 2021, the selected offices' internal controls were all functioning effectively and operating as intended. Some of these controls include ensuring taxpayer information is only shared when authorized with properly authenticated individuals, and that any disclosures are reported immediately upon discovery in accordance with *Internal Revenue Manual* procedures.[62]

Based on interviews with the selected offices, we found that officials in all five selected offices were generally aware of IRS's policies and procedures for protecting taxpayer information and what to do in the event there is a UNAX or unauthorized disclosure incident. For example, officials from all five selected offices outlined actions such as reporting the incident to TIGTA and removing an employee's access to taxpayer information if that employee was being investigated for a UNAX incident.

IRS Employees Met Completion Goals for UNAX-Related Training

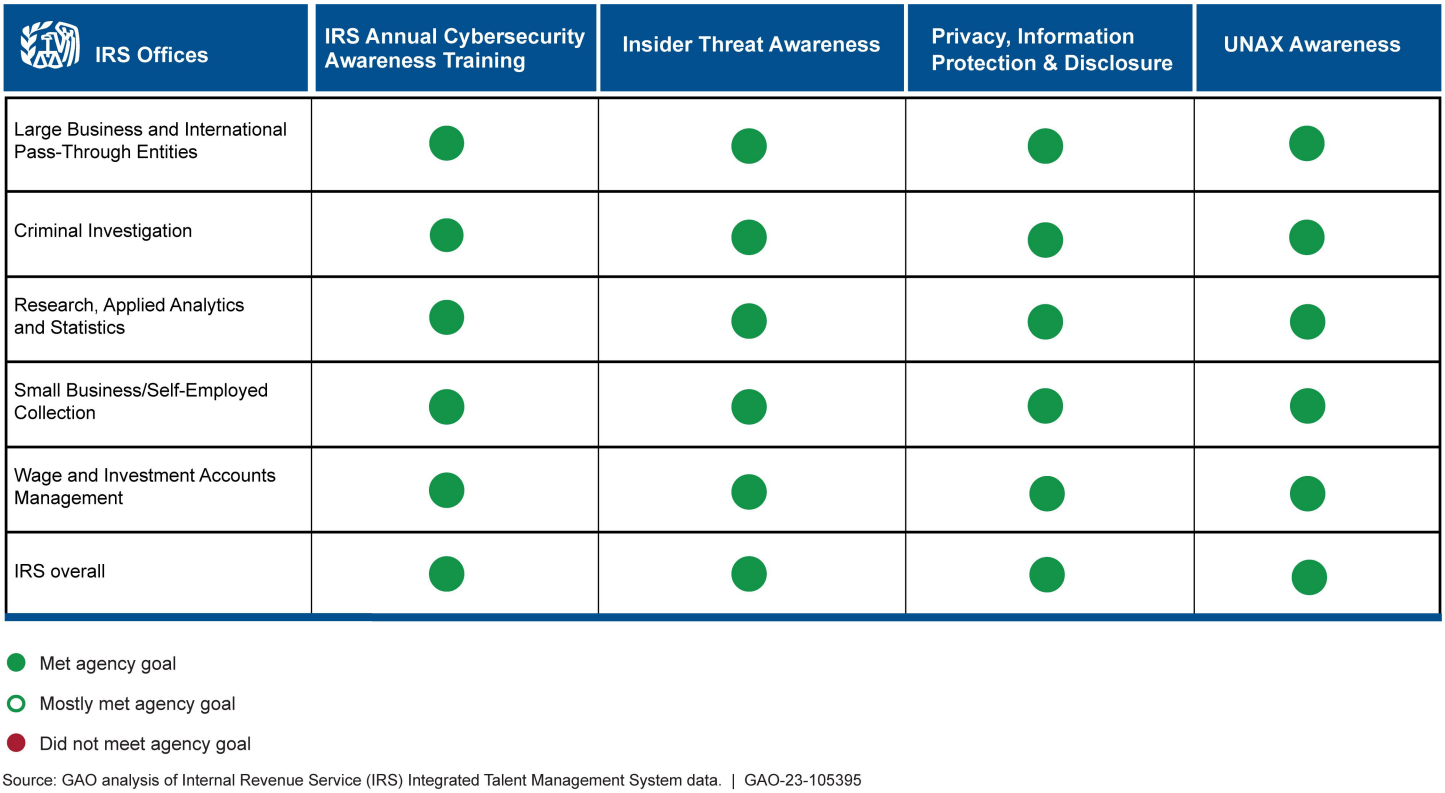
IRS requires employees to take multiple training courses related to protecting taxpayer information.[63] Training assists agencies in achieving their mission and goals by improving individual and, ultimately, organizational performance.

[62]All managers are directed to conduct an annual self-assessment of their internal controls. Managers review the effectiveness of controls within their own area of responsibility and verify that adequate management controls are in place and functioning effectively to accomplish organizational goals and protect IRS resources. We did not assess IRS's responses or process for completing this assessment as part of our work. We reviewed the results of our recent audits of IRS's financial statements, including our subsequently issued management reports presenting new deficiencies in IRS's internal control over financial reporting and the status of IRS's corrective actions to address prior deficiencies. GAO, *Financial Audit: IRS's FY 2022 and FY 2021 Financial Statements*, GAO-23-105564 (Washington, D.C.: Nov. 10, 2022); *Management Report: IRS Needs to Improve Financial Reporting and Information System Controls*, GAO-22-105559 and GAO-22-105558SU (Limited Official Use Only version) (Washington, D.C.: May 25, 2022); and *Financial Audit: IRS's FY 2021 and FY 2020 Financial Statements*, GAO-22-104649 (Washington, D.C.: Nov. 10, 2021).

[63]We identified mandatory training courses related to protecting taxpayer information. Of these courses, IRS employees are required to take four annually: IRS Annual Cybersecurity Awareness Training; Insider Threat Awareness; Privacy, Information Protection & Disclosure; and UNAX Awareness. These courses were IRS's required courses for fiscal year 2021. For more information on how we identified these training courses, see appendix I.

IRS has an agency-wide employee training completion goal of 97 percent for all training courses. As shown in figure 4, all five of the selected offices, as well as all IRS employees, met the goal in fiscal year 2021.

Figure 4: IRS Employee Training Completion Rate by Selected Office and IRS Overall, Fiscal Year 2021



Source: GAO analysis of Internal Revenue Service (IRS) Integrated Talent Management System data. | GAO-23-105395

Accessible Data for Figure 4: IRS Employee Training Completion Rate by Selected Office and IRS Overall, Fiscal Year 2021

IRS office	IRS Annual Cybersecurity Awareness Training (percentage)	Insider Threat Awareness (percentage)	Privacy, Information Protection and Disclosure (percentage)	UNAX Awareness (percentage)
Large Business and International Pass-Through Entities	100	100	100	100%
Criminal Investigation	99	99	99	99
Research, Applied Analytics and Statistics	100	100	100	100
Small Business / Self-Employed Collection	100	100	100	100
Wage and Investment Accounts Management	99	99	99	99

IRS office	IRS Annual Cybersecurity Awareness Training (percentage)	Insider Threat Awareness (percentage)	Privacy, Information Protection and Disclosure (percentage)	UNAX Awareness (percentage)
IRS overall	99	99	99	99

Source: GAO analysis of Internal Revenue Service (IRS) Integrated Talent Management System data. | GAO-23-105395

Note: UNAX is the willful unauthorized access, attempted access, or inspection of federal tax information. The employee training completion goal set by IRS is 97 percent. We define mostly met as within 10 percentage points of the goal (e.g., 87 to 96 percent for IRS employee training courses), and not met as anything below the mostly met range.

IRS Could Improve Oversight of Contractors

IRS Has Not Established a Contractor Training Completion Goal and Completion Rates Are Well below Those of IRS Employees

For the five courses we identified relating to protecting taxpayer information for contractors, IRS contractors' completion rates ranged from 61 percent to 74 percent for fiscal year 2021, which were well-below that of IRS employees for their required courses, as shown in table 3.[64]

Table 3: IRS Overall Contractor Training Completion Rate, Fiscal Year 2021

Training Course	Number of Contractors Assigned Training	Number of Contractors Completed Training
Insider Threat	14,068	9,270 (65.9 percent)
Inadvertent Sensitive Information Access	2,377	1,458 (61.3 percent)
Introduction to UNAX	11,731	8,129 (69.3 percent)
Privacy, Information Protection & Disclosure	11,731	8,103 (69.1 percent)
IRS Annual Cybersecurity Awareness Training	8,355	6,219 (74.4 percent)

Source: GAO analysis of Internal Revenue Service (IRS) Integrated Talent Management System data. | GAO-23-105395

Note: UNAX is the willful unauthorized access, attempted access, or inspection of federal tax information.

IRS's *Acquisition Policy* states that all contractors assigned to a contract with staff-like access to sensitive but unclassified information, including taxpayer information, must complete IRS-provided privacy and security awareness training, including the Privacy, Information Protection &

[64]IRS officials explained that not all IRS contractors have access to IRS systems. IRS provided us with a list of contractors who had been assigned to the trainings. We used the field indicating whether the training was assigned to determine the population of contractors required to complete the trainings and then the status of whether the contractor was compliant or not to calculate the completion rates. We confirmed our approach with IRS officials. These courses we identified are Insider Threat Awareness Briefing; Inadvertent Sensitive Information Access; Introduction to Unauthorized Access Briefing for IRS Contractors; Privacy, Information Protection & Disclosure Briefing; and IRS Annual Cybersecurity Awareness Training. For more information on how we identified these courses and descriptions of them, see appendix I.

Disclosure training.[65] According to IRS policy, contractors cannot be cleared to access taxpayer information without completing all annual training and are directed to ensure this training is completed.

According to IRS officials from the four selected offices who work with contractors who access taxpayer information, when a contractor is not up to date on UNAX training, IRS will disable the contractor's system access. Officials from one of those offices explained that this access is disabled until the contractor completes the required training. Additionally, according to IRS *Acquisition Policy*, the contractor may be subject to suspension, revocation, or termination of staff-like access to IRS IT systems and facilities when training is not completed.[66]

We found that IRS has not established an agency-wide goal for contractor training completion rates and does not have centralized oversight of contractor training, which could contribute to IRS contractors' training completion rates.

Lack of training completion goal. IRS does not have an agency-wide goal for contractor training completion rates. According to IRS officials, they strive for a 100 percent completion rate; however, they did not state that this was a documented goal.[67] Additionally, as discussed below, IRS's IT Cybersecurity office, whose responsibilities apply to only a

[65]Contractors required to take the Unauthorized Access to Taxpayer Data training must attest to understanding the penalties for unauthorized access, as instructed by the contracting officer representative (COR). CORs monitor contracts, perform administrative actions, and ensure the contractors under the contract complete required trainings (e.g., Privacy, Information Protection & Disclosure training).

[66]Internal Revenue Service, *Internal Revenue Service Acquisition Policy*, Publication 5488 (June 2021).

[67]The Federal Information Security Modernization Act of 2014 (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over federal agency operations and assets. In accordance with their respective responsibilities under FISMA, each agency is required to develop, document, and implement an information security program that, among other things, includes security awareness training to inform personnel, including contractors, of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security. At IRS, the Chief Information Security Officer is responsible for ensuring IRS personnel, contractors, and others receive information security awareness training and, if they have significant security responsibilities, role-based training.

subset of contractors, has a training completion goal of 90 percent for a subset of training courses, but it does not apply to all IRS contractors.

According to the *Standards for Internal Control in the Federal Government*, agencies are to define objectives clearly. Defining objectives in measurable terms enables agencies to assess performance toward achieving them and establish activities to monitor these performance measures.[68]

Without a set agency-wide goal for contractor training, IRS has no measure to use to assess contractor training completion rates. A goal would help IRS better monitor contractors' training compliance and identify when corrective action may be needed. This would help IRS ensure contractors meet their training requirements and know how to properly protect taxpayer information.

Lack of centralized oversight. Several IRS offices are involved in monitoring contractor training; however, IRS did not identify any centralized office that monitors all contractor training completion. IT Cybersecurity officials said the absence of a single office that monitors contractor training also contributes to the low contractor training completion rate. As shown in table 4, IRS's IT Cybersecurity, Facilities Management and Security Services, and Human Capital Offices all have a role in the monitoring and oversight of contractors.

Table 4: IRS Offices Involved in Overseeing Aspects of Contractor Training, as of December 2022

IRS Office	Responsibilities Related to Contractor Training Oversight
IT Cybersecurity office	According to IT Cybersecurity officials, as part of their Federal Information Security Modernization Act of 2014 (FISMA) responsibilities, they monitor training metrics on a portion of IRS contractors; however, they are not responsible for monitoring training metrics on all contractors. According to officials, in addition to monitoring trends on these training courses, the Cyber Mandatory Security Training Program office monitors and communicates training completion rates for the Privacy, Information Protection & Disclosure, UNAX and Inadvertent Sensitive Information Access training courses, among other training courses, for contractors with active IRS network accounts. IT Cybersecurity officials said that they found their training monitoring to be successful in ensuring contractors with active IRS network accounts met their training requirements for FISMA required trainings, including the Cybersecurity Awareness and Insider Threat Awareness training courses. According to officials, the subset of contractors whose training completion they were monitoring have met the IT Cybersecurity office's goal of 90 percent each year since 2017.

[68]GAO-14-704G.

IRS Office	Responsibilities Related to Contractor Training Oversight
Facilities Management and Security Services office	According to IRS officials, IRS's Facilities Management and Security Services office's role is to track contractors' completion of a subset of training, the Security Awareness training courses, and remove contractors' access to IRS buildings if they do not complete the required trainings. However, this office does not monitor other contractor training or remove access to IRS equipment or systems if contractors do not complete required training.
Human Capital Office	The Human Capital Office's Contractor Security Management office facilitates and tracks contractor onboarding and separation activities. However, the office does not track Security Awareness training.

Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-23-105395

Note: The Security Awareness training courses include the Cybersecurity Awareness; Privacy, Information Protection & Disclosure; Unauthorized Access to Taxpayer Data; Inadvertent Sensitive Information Access; and Insider Threat trainings. All these train employees on how to properly protect taxpayer information.

IRS officials said they are taking steps to address some gaps in contractor oversight. First, IRS's Office of the Chief Procurement Officer is leading the development of an Enterprise Contract Oversight Center, a multidisciplinary central location for contract oversight collaboration and guidance. Second, according to IRS officials, the agency began transitioning the responsibility of tracking contractor training to IRS's Human Capital Office's Mandatory Briefings office in October 2022. The Enterprise Contract Oversight Center is also intended to help with this transition. IRS officials said this office will distribute contractor training completion reports to contracting officer representatives (COR) and contractors, similar to how the Human Capital Office oversees IRS employee training completion.

However, IRS was unable to provide documentation of the Human Capital Office's role or responsibilities in overseeing contractor training compliance. According to the *Standards for Internal Control in the Federal Government*, agencies are to implement control activities through policies. Documenting offices' responsibilities, including the timing of control activities and any follow-up corrective actions to be performed if deficiencies are identified, helps enable staff to implement control activities and allow management to effectively monitor those activities.[69]

If IRS contractors do not complete required training, they have an increased risk of not being prepared to handle taxpayer information and create administrative burdens. Officials from the Office of the Chief Procurement Officer told us that the process of removing and reinstating contractors' access to taxpayer information is an administrative burden.

[69]GAO-14-704G.

Additionally, officials told us that the reinstatement process can take time and could negatively affect project milestones.

Monitoring the contractor training completion rates will let IRS know when contractors are not meeting their training requirements, so it can take appropriate action to help ensure they complete the briefings. This, in turn, will help ensure contractors are equipped with the knowledge and skills to properly handle taxpayer information. Additionally, increased contractor training completion rates will reduce the administration burden on IRS officials that are to disable contractors' access to systems when the contractors do not complete the required training.

Documenting IRS's plan for the Human Capital Office to fulfill this role will help ensure controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated. Having the Human Capital Office as a centralized point to monitor contractors could help achieve contractor compliance with training requirements. It could also help them understand how to properly protect taxpayer information, as well as reduce the burden of contractors' access being disabled and re-enabled.

Some IRS Officials Responsible for Overseeing Contractors Did Not Know How to Report Incidents

CORs help provide oversight of contractors, including ensuring that contractors are aware of data safeguards and are appropriately protecting taxpayer information. According to IRS officials, CORs receive training prior to being approved for their respective positions. Additionally, according to the *Internal Revenue Manual* certain employees, including CORs, are to receive annual security and privacy training.[70] IRS also provides guidance outlining CORs' responsibilities for reporting UNAX and unauthorized disclosure incidents.

Contracting Officer Representatives (COR)

CORs are IRS employees who oversee day-to-day operations of contracts and contractors. COR responsibilities include:

- Ensuring that contractors complete required training
- Ensuring contracts are performed as written
- Ensuring contractors are aware of data safeguards and are appropriately protecting taxpayer information
- Monitoring contractor technical performance
- Reporting potential or actual problems to the contracting officer—an official in IRS's Office of the Chief Procurement Officer responsible for modifying or terminating a contract and making determinations and findings related to the contract

According to officials, CORs receive specific training prior to being approved for their respective positions.

Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-23-105395

IRS Publication 4812, *Contractor Security & Privacy Controls: Handling and Protecting Information or Information Systems* instructs CORs to report incidents to the contracting officer, IRS's Computer Security Incident Response Center, and, when appropriate, the Situational Awareness Management Center.[71] According to this guidance, CORs should report incidents to the Computer Security Incident Response Center within one hour of becoming aware of the incident. IRS's Insider Threat Awareness Briefing instructs employees to report incidents that can include UNAX or unauthorized disclosure to the Situational Awareness Management Center within a half hour of the incident discovery or when it is safe to do so.

The CORs for the four selected offices working with contractors accessing taxpayer information had mixed awareness of what to do if there was a UNAX or unauthorized disclosure incident, or if a UNAX or

[70]Internal Revenue Service, *Internal Revenue Manual* § 10.8.1.3.2.2 AT-3 Role-Based Training (Sept. 28, 2021), and *Internal Revenue Manual* § 10.8.2.2.1.10.1 Contracting Officers Representatives (COR) (Sept. 5, 2012).

[71]The Computer Security Incident Response Center is responsible for preventing, detecting, reporting, and responding to cybersecurity incidents. The Situational Awareness Management Center is responsible for documenting and reporting incidents, threats, and emergencies.

unauthorized disclosure case was substantiated, as shown in table 5.[72] Some of the CORs we met with did not always name all parts of the process for responding to incidents and violations. Also, when asked about reporting requirements, not all CORs identified the proper offices to report incidents. Additionally, CORs from one office said they were not aware of what steps to take if a UNAX incident was substantiated.

Table 5: Selected Offices' Contracting Officer Representatives' Awareness of UNAX Reporting Requirements

Category	Complete Computer Security Incident Reporting Form within one hour	Contact Computer Security Incident Response Center	Contact Situational Awareness Management Center	Report to Contracting Officer
Office 1	Yes	Yes	Yes	Yes
Office 2	No	Yes	Yes	Yes
Office 3	Yes	No	No	No
Office 4	No	No	No	No

Source: GAO analysis of interviews with Internal Revenue Service (IRS) officials. | GAO-23-105395

Note: UNAX is the willful unauthorized access, attempted access, or inspection of federal tax information. We selected five IRS offices to understand how they protect taxpayer information and the challenges they face in doing so. Offices 1-4 in the table above are four of our selected offices: Criminal Investigation; Large Business and International Division's Pass-Through Entities office; Office of Research Applied Analytics, and Statistics; and Small Business/Self-Employed Division's Collection office. However, the offices are kept anonymous. According to IRS officials, the fifth selected office, the Wage & Investment Division's Accounts Management office, does not work with contractors with staff-like access to taxpayer information. We did not interview any contracting officer representatives from this office.

IRS officials said CORs may not be aware of the reporting requirements for several reasons. First, although the Insider Threat Awareness Briefing—one of IRS's annual mandatory training courses for all employees—provides information on how to report UNAX incidents, it is not a COR-specific training and does not focus on CORs' roles related to their duties. Additionally, officials noted that many COR processes are not documented and it can be difficult to locate COR-related guidance. Finally, taking action on a substantiated UNAX case is not a routine or daily function and IRS Procurement officials believe there is a need for an annual refresher training on COR-related duties.

[72]We met with CORs in Criminal Investigation, the Large Business and International Division, the Office of Research, Applied Analytics, and Statistics, and the Small Business/Self-Employed Division Collection office. All of these selected offices have contractors with access to taxpayer information. According to IRS officials, the fifth selected office, the Wage & Investment Division (W&I) Accounts Management office, does not work with contractors with staff-like access to taxpayer information. We did not interview any W&I Accounts Management CORs.

If IRS CORs are not fully aware of where or how to report UNAX or unauthorized disclosure incidents, IRS has limited assurance that it will be able to provide appropriate and timely responses to incidents involving taxpayer information. Additionally, IRS might not be receiving full or accurate information related to UNAX or unauthorized disclosure incidents if these reporting requirements are not correctly followed.

As mentioned previously, IRS is developing the Enterprise Contract Oversight Center. In addition to the duties mentioned above, the center will establish oversight, policy, processes, and compliance efforts to help CORs better understand their duties. The Center will serve as a central location for contractor oversight guidance. It will also facilitate collaboration with IRS offices for tracking contractor oversight. Officials explained that this Center will provide CORs with information on UNAX incidents and what they should do if an incident occurs. IRS plans to focus on updating annual COR training and developing guidance for CORs, such as process maps, among other things, in fiscal years 2023 and 2024.

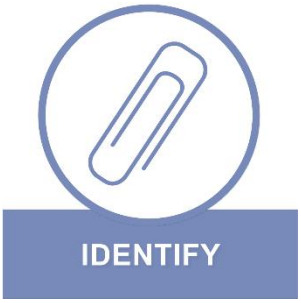
While one of the intended goals of the Enterprise Contract Oversight Center is to increase CORs' awareness on reporting UNAX incidents, the Center is still being organized. Therefore, training has not been updated and guidance has not been developed. Ensuring the Center updates and develops necessary training and guidance for CORs on reporting UNAX and unauthorized disclosure incidents can help better ensure CORs know their reporting requirements.

IRS Has Opportunities to Improve Monitoring of UNAX Cases

IRS's monitoring of UNAX prevention efforts is limited by its incomplete inventory of systems that process or store taxpayer information. The lack of completeness limits IRS's visibility into all of its systems that store and process taxpayer information. The incomplete inventory also hamstrings the Privacy, Governmental Liaison and Disclosure (PGLD) office's ability to target training and monitor UNAX case trends because PGLD does not have important contextual information—the number of employees authorized to access taxpayer information. Additionally, IRS does not monitor trends of IRS contractor UNAX cases.

IRS Monitoring of UNAX Prevention Efforts Is Limited by an Incomplete Inventory of Systems that Process or Store Taxpayer Information

Agencies are required to develop and maintain an inventory of major information systems.[73] A complete and accurate inventory of major information systems is a key element of managing agency information technology resources, including the security of those resources. The inventory is an important tool in tracking agency systems for oversight, as well as implementing and assessing security controls.



IRS policy aligns with Office of Management and Budget implementation guidance and National Institute of Standards and Technology (NIST) guidance.[74] This policy directs the agency to develop and maintain an inventory of all systems that process personally identifiable information, such as taxpayer information.[75] The IT office, in collaboration with PGLD, is responsible for managing IRS's system inventory. PGLD is responsible for identifying and documenting whether IRS's systems, applications, and databases contain personally identifiable information or taxpayer information. The IT Cybersecurity office is to evaluate this information to determine what safeguards are needed to protect this sensitive information, among other things.

IRS has taken steps to develop and maintain an inventory of systems that process or store personally identifiable information and taxpayer information; however, IRS has not completed the inventory. As of December 2022, our review identified seven information systems that IRS omitted from its inventory. According to IRS officials from our selected offices, these omitted systems process or store taxpayer information. Our review also identified inventory entries for 118 systems that were not

[73]44 U.S.C. § 3505(c); The Office of Management and Budget provides guidance for agencies to follow in meeting these statutory requirements. Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016), 5. An information system is a discrete set of information resources organized for the collection, maintenance, or disposition of information. 44 U.S.C. § 3502(8).

[74]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016), 5. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020), 206.

[75]Internal Revenue Service, *Internal Revenue Manual* § 10.8.1.3.13.5, System Inventory (Dec. 13, 2022).

complete. Specifically, the entries did not establish whether the systems process or store personally identifiable information or taxpayer information.

According to IRS officials, the agency's inventory of systems is maintained, in part, using automated procedures. These procedures access and retrieve system information from a variety of sources, including authoritative databases maintained by IT and PGLD that identify IRS systems that process or store taxpayer information. In some cases, these databases contain incorrect information about systems that process or store taxpayer information, which results in an incomplete system inventory.

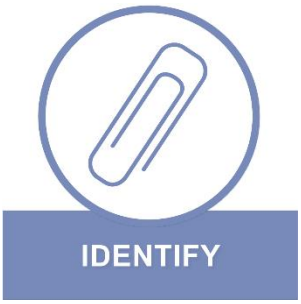
The Treasury Inspector General for Tax Administration (TIGTA) has also reported on IRS's challenges with developing and maintaining a comprehensive system inventory. For example, in July 2022, TIGTA reported that IRS could improve on maintaining an accurate and comprehensive inventory of its information systems.[76]

Ensuring that system information is accurate will help IRS maintain a comprehensive inventory of systems that process or store taxpayer information. Maintaining a comprehensive system inventory will help IRS ensure it has implemented safeguards to protect taxpayer information being processed or stored on all of its systems, applications, and databases. Further, having a comprehensive inventory would enable IRS to monitor all relevant IT systems—systems that process taxpayer information—to detect if its staff access taxpayer information without authorization.

[76]Treasury Inspector General for Tax Administration, *Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation*, 2022-20-040 (Washington, D.C.: July 18, 2022).

IRS Could Better Target Resources and Monitor UNAX Case Trends with More Complete Analysis

PGLD monitors the number of UNAX cases and associated trends by analyzing data to identify groups of IRS employees within certain parts of IRS that have lower and higher rates of UNAX investigations relative to their proportion of the IRS population. According to PGLD officials, their analysis helps them determine where to target UNAX prevention efforts, including training and communications.



When analyzing UNAX case characteristics, PGLD compares the percentage of all employees in certain groups (e.g., IRS business unit or office) or with certain characteristics (e.g., length of time employees have been federal employees) to the percentage of UNAX cases in those groups. For example, PGLD found that the Wage & Investment Division (W&I) Service Center employees represented 35 percent of the overall IRS population, but made up 57 percent of IRS UNAX investigations for fiscal year 2021.[77] Conversely, PGLD's analysis also found that several business units with UNAX cases totaled 32 percent of the overall IRS population, but made up 6 percent of IRS UNAX investigations.[78]

However, PGLD's analysis does not consider important contextual information. Namely, the analysis does not include the number of employees authorized to see taxpayer information. These calculations could miss identifying a business unit with a relatively low rate of UNAX cases out of all employees but a relatively high rate out of the number of IRS employees actually accessing taxpayer information. In the example described above, it would appear that employees in the W&I Service Centers have much higher rates of UNAX case investigations than their proportion of the agency-wide population. However, according to W&I officials, Service Center employees need to access taxpayer information daily to process tax returns and provide taxpayers with information on the

[77]As we reported in May 2022, many W&I employees work in job functions that necessitate access to federal tax information, especially staff in the Service Centers. W&I Service Centers house different functions, including answering tax law and tax account inquiries and adjusting tax accounts. For more information, see GAO-22-105872.

[78]PGLD's analysis grouped the following IRS business units together for this calculation: Independent Office of Appeals, Office of the Chief Financial Officer, Criminal Investigation, Human Capital Office Office of HR Operations, IT, LB&I, Office of Professional Responsibility, Small Business/Self-Employed Division (SB/SE) Office of Fraud Enforcement, SB/SE Operations Support, SB/SE Service Center, and the Tax-Exempt and Government Entities Division.

status of their returns and refunds. These employees use an IRS IT system that gives staff the ability to have instantaneous view of certain taxpayer information. Conversely, according to IRS officials, the majority of Criminal Investigation employees are given access to taxpayer information pertinent to specific tax cases and do not have the ability to access taxpayer information through that IT system.

According to the *Internal Revenue Manual*, PGLD is to work to prevent UNAX violations and identify ways to improve the UNAX Program's effectiveness.[79] According to federal internal control standards, agencies are to use quality information that is appropriate, current, complete, accurate, accessible, and timely to make informed decisions and evaluate performance in achieving key objectives and addressing risks.[80]

In addition, according to our guidance on designing evaluations, differences in populations can explain differences in effectiveness.[81] The guidance also states that one consideration for the appropriateness of data is whether variation in data across locations precludes making reliable comparisons. For example, differing rates of UNAX cases across offices may be due to differing numbers of IRS employees authorized to access taxpayer information. Without this relevant information, it can be difficult to identify actions to improve program performance.

As of December 2022, PGLD did not have information on the number of IRS employees authorized to see taxpayer information overall or by business unit. PGLD also does not have information on the number of employees routinely accessing taxpayer information by business unit. A complete listing of systems that store or process taxpayer information, as discussed above, would provide PGLD with the ability to identify the number of employees authorized to access taxpayer information in each business unit.

PGLD would have a more complete and well-rounded view of IRS employee UNAX case trends if it considered where there is a high rate of UNAX based on the number of IRS employees authorized to access

[79]Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.1, IRP UNAX Program Office Roles and Responsibilities (Mar. 8, 2023), and *Internal Revenue Manual* § 10.8.1.3.1.1.8.1, Unauthorized Access (UNAX) (May 9, 2019).

[80]GAO-14-704G.

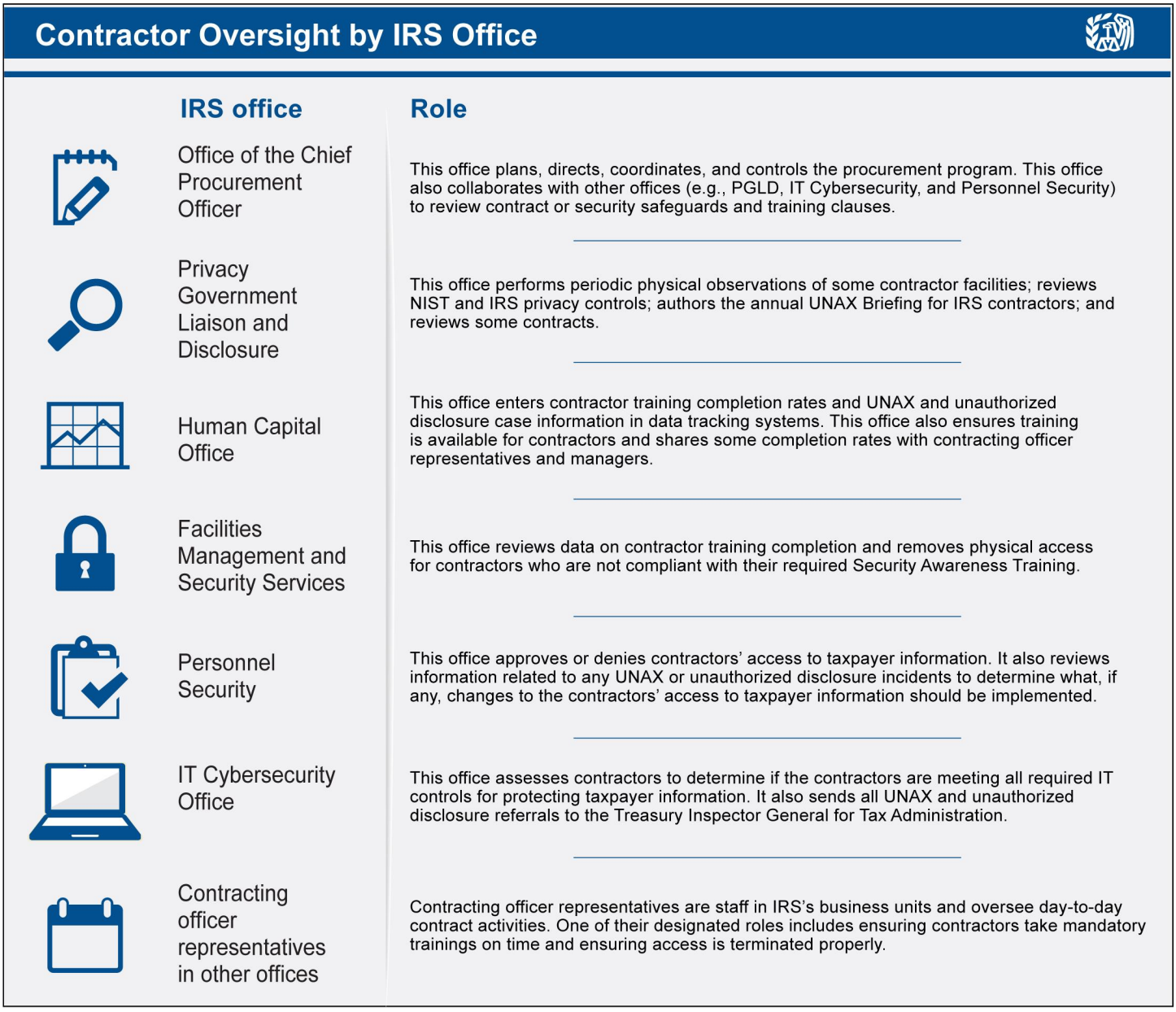
[81]GAO, *Designing Evaluations: 2012 Revision (Supersedes PEMD-10.1.4),* GAO-12-208G (Washington, D.C.: Jan. 31, 2012).

taxpayer information, in addition to considering where there is a high rate of UNAX cases out of all employees. PGLD could better target its resources and determine the effectiveness of the agency-wide UNAX program. For example, PGLD would be better able to discern if changes in case amounts or characteristics are because the size of IRS's workforce changed or if one business unit became better or worse at protecting taxpayer information. This is especially important as IRS's staffing levels or organizational structure could change in response to changes in legislation or funding levels.

IRS Does Not Monitor Trends in IRS Contractor UNAX and Unauthorized Disclosure Cases

Various offices within IRS have some role in overseeing contractors; however, we found that IRS does not do any centralized monitoring of contractor UNAX and unauthorized disclosure cases. This gap leads to limited insight into contractor UNAX and unauthorized disclosure trends. As shown in figure 5, IRS contractor oversight is spread across several IRS offices. PGLD does not track, monitor, and analyze data on UNAX and unauthorized disclosure cases for contractors as it does for employees.

Figure 5: Contractor Oversight by IRS Office as of December 2022



Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-23-105395

Accessible Data for Figure 5: Contractor Oversight by IRS Office as of December 2022

IRS office	Role
Office of the Chief Procurement Officer	This office plans, directs, coordinates, and controls the procurement program. This office also collaborates with other offices (e.g., PGLD, IT Cybersecurity, and Personnel Security) to review contract or security safeguards and training clauses.
Privacy Government Liaison and Disclosure	This office performs periodic physical observations of some contractor facilities; reviews NIST and IRS privacy controls; authors the annual UNAX Briefing for IRS contractors; and reviews some contracts.
Human Capital Office	This office enters contractor training completion rates and UNAX and unauthorized disclosure case information in data tracking systems. This office also ensures training is available for contractors and shares some completion rates with contracting officer's representatives and managers.
Facilities Management and Security Services	This office reviews data on contractor training completion and removes physical access for contractors who are not compliant with their required Security Awareness Training.
Personnel Security	This office approves or denies contractors' access to taxpayer information. It also reviews information related to any UNAX or unauthorized disclosure incidents to determine what, if any, changes to the contractors' access to taxpayer information should be implemented.
IT Cybersecurity office	This office assesses contractors to determine if the contractors are meeting all required IT controls for protecting taxpayer information. It also sends all UNAX and unauthorized disclosure referrals to the Treasury Inspector General for Tax Administration.
Contracting officer representatives in other offices	Contracting officer representatives are staff in IRS's business units and oversee day-to-day contract activities. One of their designated roles includes ensuring contractors take mandatory trainings on time and ensuring access is terminated properly.

Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-23-105395

Note: UNAX is the willful unauthorized access, attempted access, or inspection of federal tax information. PGLD is the Privacy, Government Liaison, and Disclosure office. NIST is the National Institute of Standards and Technology.

According to the *Internal Revenue Manual*, PGLD is responsible for a comprehensive agency-wide UNAX program that includes education and compliance for all IRS staff—employees and contractors. Also, according to the *Internal Revenue Manual*, PGLD is to work to prevent UNAX violations and identify ways to improve the UNAX Program's effectiveness.[82] *Standards for Internal Control in the Federal Government* states that agencies should monitor internal control and use that information, along with any other evaluations, to evaluate the controls, and determine appropriate corrective actions for deficiencies on a timely basis.[83]

PGLD officials told us they do not do any agency-wide monitoring of IRS contractor UNAX cases because the data the office uses to analyze IRS

[82]Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.1, IRP UNAX Program Team Roles and Responsibilities (July 10, 2018).

[83]GAO-14-704G.

employee UNAX case amounts and trends—data from IRS's Automated Labor and Employee Relations Tracking System—do not include information on IRS contractor UNAX and unauthorized disclosure cases.

IRS has data on IRS contractor UNAX and unauthorized disclosure cases in a different system—e-Trak Reports of Investigation Unit—but it would be of limited use in analyzing overall case amounts and trends. E-Trak Reports of Investigation Unit includes a tracking and retention database for all investigations that TIGTA refers to IRS, which includes all UNAX cases. Some of the information that IRS uses to track these cases could be used to monitor overall IRS contractor UNAX and unauthorized disclosure case amounts and trends (e.g., date received from TIGTA). However, this system is designed for case management and collects information for that purpose and may have limited effectiveness for monitoring contractors.

Based on our analysis, e-Trak UNAX and unauthorized disclosure case data have limitations in reliability and content that could make monitoring overall IRS contractor UNAX and unauthorized cases difficult. When we compared data from both the Automated Labor and Employee Relations Tracking System and the e-Trak system on IRS employee cases, we identified discrepancies that we could not resolve. For example, the number of IRS employee UNAX cases in the Automated Labor and Employee Relations Tracking system and the e-Trak system did not match for fiscal years 2016 through 2021.

In addition, we found that the e-Trak system has data content limitations that prevent IRS from using the e-Trak data to determine all contractor UNAX and authorized disclosure cases and whether a case was substantiated. For example, we found the field where contractor status could be entered included blank values. We also found instances where the contractor case data did not provide information on contractor status. For example, individuals listed in the contractor dataset were categorized as IRS employees or former employees. Additionally, according to IRS officials, the e-Trak system was not designed to track issue substantiation.

According to federal internal control standards, management should use quality information—information that is appropriate, current, complete, accurate, accessible, and timely—to make informed decisions and

evaluate the agency's performance in achieving key objectives and addressing risks.[84]

Without effective monitoring of contractors, IRS is not aware of the full extent of contractor UNAX and unauthorized disclosure cases and violations. It could underestimate or overestimate the problem and assumes greater risk of missing opportunities to improve the UNAX Program's effectiveness and further prevent UNAX violations.

[84]GAO-14-704G.

Gaps in IT Controls Present Risks to Taxpayer Information

IRS Is Implementing New Logging and Monitoring Controls on a System that Processes Taxpayer Information

IRS's IT Cybersecurity office is responsible for protecting taxpayer information from internal and external cyber-related threats, and as part of those efforts, the office enforces logging and monitoring activities of IRS's IT systems. Logging and monitoring activities enable agencies to detect and investigate security events to determine information about actions that have been taken on a system—what happened, when it happened, and who did it. Logging and monitoring involve the regular collection and review of security events for indications of inappropriate or unusual activity and the appropriate investigation and reporting of such activity.

IRS implemented controls to identify instances when its staff access taxpayer information without authorization on some, but not all, IRS systems that process taxpayer information. IRS staff are responsible for accessing taxpayer information only when it is required to complete official IRS duties as assigned. If IRS staff access taxpayer information that is not a part of their assigned duties, or is otherwise prohibited, then this access is unauthorized. Further, in some instances, business units share taxpayer information from a system with controls to a system without these control activities. IRS has not implemented processes to log and monitor when staff access taxpayer information without authorization on this system without these safeguards.

NIST recommends that agencies enable event-logging features in their information systems and retain sufficient logs to support the monitoring of events that are significant and relevant to the security of systems and the privacy of individuals.[85] NIST also recommends that agencies establish automated mechanisms to collect and analyze data for increased threat and situational awareness. As part of this, agencies should have an

[85]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020), 66.

automated centralized event analysis capability that provides event aggregation and correlation capabilities and alerting mechanisms.[86]

Consistent with NIST guidance, IRS policy requires events that are significant and relevant to protecting taxpayer information to be logged. IRS policy also requires automated mechanisms to be used to integrate event review, analysis, and reporting processes. The IT Cybersecurity office is to manage a centralized capability to evaluate events and identify potential UNAX violations. Further, the IT Cybersecurity office is to refer potential UNAX violations to TIGTA for investigation and then work with IRS management to incorporate feedback related to the potential violations.

According to IT Cybersecurity officials, IRS has activities underway to implement new controls intended to expand its logging capabilities and monitor for instances when its staff access taxpayer information on this system without authorization. However, some challenges in IRS's ability to implement the controls have led to delays. IRS plans to have these new logging and monitoring controls implemented in July 2024.

IRS Has Not Developed Security Documentation for One System as Directed by Federal Guidance

According to NIST guidance, organizations should develop system security plans to improve the protection of information system resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to

[86]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020), 200.

meet those requirements.[87] NIST guidance also recommends that agencies' information systems have a security authorization.[88]

IRS developed procedures in September 2010 for ensuring new and existing systems are properly and accurately classified and accounted for in the agency's list of systems that must adhere to FISMA.[89] As part of this process, a system's points of contact are required to complete a system inventory classification checklist for each of their systems to describe each system and help in determining the classification of the systems. Subsequent to completing the classification process, these procedures require IRS to develop an authorization to operate and a system security plan, among other things, as appropriate, for the system and be accounted for in its list of systems that are to adhere to FISMA.

As of December 2022, one of the five selected IRS systems we reviewed has not gone through IRS's process to determine if it is accurately classified and accounted for in the agency's FISMA system inventory. This system is used by the Large Business and International Division's (LB&I) Pass-Through Entities office to track affluent taxpayers' risk of tax noncompliance and document IRS's risk assessment of their potential noncompliance. IRS has not identified whether it is required to develop appropriate security assessment and authorization documents for this LB&I system. For example, IRS has not developed an authorization to operate or a system security plan for it.[90] This LB&I system has been operating without these security assessment and authorization

[87]National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18 (Gaithersburg, MD: February 2006), vii, and *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020), 417.

[88]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018), x. A security authorization is the decision given by a senior official to put an information system into operation, based on a defined system boundary, and to explicitly accept the risk to the organization.

[89]Internal Revenue Service, *Federal Information Security Management Act (FISMA) Master Inventory Standard Operating Procedures,* Version 4.0 (Sept. 15, 2021).

[90]IRS has developed the security assessment and authorization documents for the other four selected systems that we reviewed.

documents since 2009, creating a risk of unauthorized access or disclosure to taxpayer information.

According to IRS officials, in 2010, IRS developed its procedures for implementing FISMA—one year after the agency created this system. Thus, the LB&I system did not go through this process. The classification checklist would help to determine whether the system is accurately classified and would be accounted for in the agency's FISMA system inventory. LB&I officials stated that they submitted an inventory classification checklist for this system on December 7, 2022—13 years after the system began collecting taxpayer information.

Until IRS completes the inventory classification process for the system used to track affluent taxpayers' risk of tax noncompliance and develops key security assessment and authorization documentation for the system, the agency will not fully understand the risks associated with operating the system. This would include developing an authorization to operate for the system. Further, until IRS prepares a system security plan, it has limited assurance that the appropriately designed security controls are designed and operating effectively to safeguard taxpayer information.

IRS Does Not Have Processes to Determine How Long Taxpayer Information Is to Reside on Two Research Systems

According to the *Internal Revenue Manual*, disposing of taxpayer information appropriately and when no longer needed helps protect taxpayer information and is required by federal law.[91] Per Office of Management and Budget guidance, IRS is to maintain personally identifiable information, including taxpayer information, in accordance with applied Records Control Schedules approved by the National Archives and Records Administration.[92] According to IRS policy, an effective records and information management program is vital to ensure information is protected.

[91]44 U.S.C. §§ 3301–3314; 36 C.F.R. §§ 1224.1–1224.10; Internal Revenue Service, *Internal Revenue Manual* § 1.15.1.2(1)(e), Authority (Feb. 5, 2021).

[92]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016), 17. Records control schedules provide mandatory instructions for the disposition of records when they are no longer required by the agency. They provide legal disposition authority for continued retention and preservation of records of historical value, among other things.

IRS establishes Records Control Schedules for its records, including electronic records (i.e., system data)—some of which contain taxpayer information—that have been approved by the National Archives and Records Administration. IRS's records management program must review and obtain National Archives and Records Administration approval for Records Control Schedule dispositions prior to their use. According to IRS records management officials, the program works with IRS business units to develop new Records Control Schedules and update existing schedules as needed.

Specifically, records management officials stated that IRS business units are to initiate and collaborate with records management officials within their organizations to publish new schedules or update existing schedules. Further, the records management program manages system data by evaluating existing systems to ensure compliance with National Archives and Records Administration electronic recordkeeping requirements.

However, we found that two research and analysis systems that store taxpayer information, the Compliance Data Warehouse (CDW) and Link Analysis Tool (YK1), retain system data longer than the retention periods authorized by the Records Control Schedules. The schedule for CDW directs IRS to delete system data 10 years after the end of the processing year or when no longer needed for operational purposes. Similarly, the schedule for YK1 directs IRS to archive system data 10 years after the end of the processing year and delete system data 16 years after the end of the processing year or when no longer needed for operational purposes. According to Office of Research, Applied Analytics, and Statistics (RAAS) Data Management Division officials, CDW and YK1 have retained system data for 25 and 19 years, respectively. Officials do not have plans to delete any system data.

The current schedules provide flexibilities to retain system data longer than the authorized periods indicated in the schedules if there is a clear operational purpose. According to RAAS officials, RAAS retains system data on CDW and YK1 indefinitely for research purposes. However, officials noted that IRS has not formally defined "operational purpose." Further, officials stated that they do not consider these systems to be operational databases but rather research systems.

According to RAAS officials, the system data are essential for tax policy research. As of September 2022, CDW had more than 1,000 active accounts and it has a wide range of users—IRS, Department of the

Treasury, Congress, and nonfederal employee researchers. Officials stated that RAAS is purchasing additional data storage to continue retaining system data beyond the current authorized retention periods.

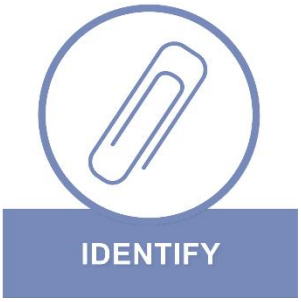
However, RAAS data management officials stated that RAAS does not have formal processes in place to determine how long system data are to be retained. Specifically, RAAS does not have documented criteria or factors to consider when determining what data are needed for operational purposes and what data can be deleted or archived per approved Records Control Schedules. RAAS officials said if they were going to consider deleting or archiving data, they would first survey known data users.

IRS is taking steps to meet National Archives and Records Administration recordkeeping requirements for CDW and YK1. As of December 2022, IRS records management officials explained that they plan to update the Records Control Schedules to ensure they accurately reflect the business need for CDW and YK1 system data. As of June 2023, RAAS officials said they are working with records management officials to update the retention schedules to reflect necessary timeframes to maximize user benefits. Officials said this policy would determine when and how data would be deleted or archived.

Until IRS implements processes to determine when taxpayer information should no longer be stored in CDW and YK1, the agency cannot be compliant with approved Records Control Schedules. Implementing such processes would allow management to make a more informed decision on accepting risk associated with retaining large amounts of taxpayer information on systems accessed by a wide range of users.

IRS Has Not Assessed the Risks of Its Method to Transfer Taxpayer Information to Contractors

According to NIST guidance, risk assessments are a key part of an effective risk management program and facilitate decision-making at the



agency, mission or business process, and information system levels.[93] Risk assessments can help to inform specific decisions such as appropriate ways of sharing data with external entities.

The *Internal Revenue Manual* requires that systems and data supporting critical operations and assets be assessed for the risk and magnitude of harm that could result from vulnerabilities and potential threats.[94] The guidance states that the risk assessment is to include identifying the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of a system and the information it processes, stores, or transmits, and any related information.

One of the five selected offices—Small Business/Self-Employed Division (SB/SE) Collection office—contracts with private collection agencies to collect tax debts IRS is not actively pursuing.[95] SB/SE shares taxpayer information electronically with private collection agencies. The private collection agencies then have access to the taxpayer information through their respective IT systems, which are not owned or managed by IRS.

SB/SE Collection officials stated that IRS conducts annual contractor security evaluations as required by IRS Publication 4812 to assess and validate the effectiveness of security controls established for contractors receiving taxpayer information to protect the agency's information and information systems.[96] However, the agency has not conducted an initial risk assessment to identify whether its method of sharing the data electronically appropriately protects taxpayer information.

[93]National Institute of Standards and Technology, *Guide for Conducting Risk Assessments,* Special Publication 800-30, Revision 1 (Gaithersburg, MD: September 2012), ix.

[94]Internal Revenue Service, *Internal Revenue Manual* § 10.8.1, Information Technology (IT) Security, Policy and Guidance (Sept. 28, 2021).

[95]In December 2015, Congress passed the Fixing America's Surface Transportation Act, which required IRS to contract with private collection agencies to collect certain tax debts. IRS had previously contracted with private debt collectors in an earlier version of this private debt collection program from 2006 through 2009. IRS began assigning inactive tax debt cases to private collection agencies in April 2017 as a result of the law. See Pub. L. No. 114-94, div. C, tit. XXXII, subtitle A, § 32102, 129 Stat. 1312, 1733–1736 (2015), *codified at* 26 U.S.C. § 6306(c).

[96]Internal Revenue Service, *Contractor Security and Privacy Controls: Handling and Protecting Information or Information Systems*, Publication 4812 (Washington, D.C.: 2019).

According to SB/SE Collection officials, the office's decision to share taxpayer information electronically with private collection agencies was based on how IRS shared such information in the prior iteration—from 2006 to 2009—of the private debt collection program. The officials also stated that the annual contractor security evaluations validate the effectiveness of security controls established to protect information systems and IRS information once the private collection agencies receive it. Thus, they have not revisited the original decision. IRS procurement officials told us that IRS does not have a supplemental policy or guidance that requires a risk assessment to be performed prior to transferring taxpayer information to contractors.

Conducting a risk assessment would allow IRS to identify any risks associated with the method of sharing taxpayer information electronically with the private collection agencies, such as the likelihood and magnitude of harm from unauthorized access, use, or disclosure. The assessment would provide IRS with more assurance that the data sharing method is an acceptable way to share taxpayer information with external entities or could identify whether any changes are needed to better protect such information.

Modifications to Statutory Authority Could Help IRS More Easily Protect Taxpayer Information

Congress has created exceptions to the confidentiality protections of taxpayer information as part of section 6103 of the Internal Revenue Code, allowing IRS to share taxpayer information with outside agencies to help administer specific programs (see table 6). For example, IRS can share information with the Department of Education for purposes of determining an applicant's eligibility for federal student financial aid.

Table 6: Examples of Authorized Disclosures of Taxpayer Information to Other Federal Agencies for Nontax Administration Purposes

Agency authorized to receive taxpayer information	Purpose of disclosure	Internal Revenue Code subsection authorizing disclosure
Department of Education	Determining eligibility for, or repayment obligations under, income-contingent or income-based repayment plans under the Higher Education Act of 1965.	6103(*l*)(13)
Department of Health and Human Services	Locating blood donors, by sharing mailing address information, who, as indicated by donated blood or products derived therefrom or by the history of the subsequent use of such blood or blood products, have or may have HIV/AIDS, to inform such donors of the possible need for medical care and treatment.	6103(m)(6)
Department of Labor Pension Benefit Guaranty Corporation	Administration of certain provisions of the Employee Retirement Income Security Act of 1974.	6103(*l*)(2)
National Archives and Records Administration	Appraisal of records for destruction or retention.	6103(*l*)(17)
National Institute for Occupational Safety and Health	Locating individuals, by sharing mailing address information, who are, or may have been, exposed to occupational hazards to determine the status of their health or to inform them of the possible need for medical care and treatment.	6103(m)(3)
Office of Personnel Management	To carry out the Federal Employees' Retirement System.	6103(*l*)(11)

Agency authorized to receive taxpayer information	Purpose of disclosure	Internal Revenue Code subsection authorizing disclosure
Social Security Administration	Verification of employment status of Medicare beneficiary and spouse of Medicare beneficiary.	6103(*l*)(12)
U.S. Department of Agriculture	Structuring, preparing, and conducting the census of agriculture pursuant to the Census of Agriculture Act of 1997.	6103(j)(5)
U.S. Customs Service	Determining correctness of any entry in audits as provided for in the Tariff Act of 1930 or taking other actions to recover any loss of revenue, collect duties, taxes, and fees, determined to be due.	6103(*l*)(14)
Federal agencies administering federal loan program	Whether or not an applicant for a federal loan program has a tax delinquent account.	6103(*l*)(3)

Source: GAO analysis of 26 U.S.C. § 6103. | GAO-23-105395

Notes: The examples in this table are instances where the Internal Revenue Service (IRS) is authorized to share taxpayer information with other federal agencies; in some instances, IRS is also authorized to share information with state and local agencies.

These examples are not exhaustive and are not necessarily the only authorized exception for an agency. For example, IRS is also authorized to share certain taxpayer information with the Department of Health and Human Services for certain other purposes. Additionally, the type of information IRS is authorized to disclose varies by exception.

In instances where Congress has authorized IRS to share taxpayer information with outside agencies through certain provisions in Internal Revenue Code section 6103, the receiving agencies are to implement data safeguards specific to protecting taxpayer information. The agencies are also subject to IRS inspections of these safeguards in accordance with Internal Revenue Code subsection 6103(p)(4).[97] As part of these inspections, agencies are to develop corrective action plans that include explanations of actions taken or that agencies plan to take to resolve any identified weaknesses.

However, in other cases—such as when authorized by taxpayers under subsection 6103(c)—IRS may share taxpayer information with other agencies, but the safeguards of the receiving agencies are not subject to the requirements of subsection 6103(p)(4), including inspection by IRS under that provision. Officials said that in these instances it is not clear whether IRS can review and ensure that the agencies have proper controls in place to protect the information. This issue has arisen when a program includes eligibility criteria, such as adjusted gross income, but section 6103 does not directly authorize disclosure of this taxpayer information to the program's administering agency.

In these instances, the agency administering the program may work with IRS to develop procedures for taxpayers to authorize IRS to share their

[97]26 U.S.C. § 6103(p)(4).

information. The administering agency may request beneficiaries to sign releases allowing IRS to disclose taxpayer information to a third party, in this case a federal agency.[98] IRS processes the release of certain taxpayer information to the agency, pursuant to a memorandum of understanding or other agreement. While Internal Revenue Code subsection 6103(a)(1) requires that federal employees protect the confidentiality of taxpayer information, subsection 6103(p)(4)'s specific requirements for protecting taxpayer information and IRS authority under that subsection to inspect those safeguards do not apply.[99] However, other requirements to protect the information, such as protections for personally identifiable information, may apply.

An example of one such instance of IRS sharing taxpayer information under subsection 6103(c) is IRS's data sharing with the U.S. Department of Agriculture's Farm Service Agency, which processes applications for certain rural housing programs.[100] Applicants must meet certain income requirements to be eligible for the program benefits. However, the statute granting the Farm Service Agency access to taxpayer data did not amend Internal Revenue Code section 6103.[101] IRS agreed to process signed taxpayer requests for release of average adjusted gross income to the U.S. Department of Agriculture upon receipt of the taxpayer's (i.e., an applicant) signed authorization pursuant to subsection 6103(c).

IRS officials said they do not routinely enter into such agreements in lieu of authorizing legislation that amends subsection 6103(*l*) to authorize

[98]IRS officials said they do not routinely enter into such agreements in lieu of authorizing legislation that amends Internal Revenue Code subsection 6103(*l*) to authorize disclosure for a nontax federal program. Officials further stated when specific federal legislation for a nontax program requires use of tax data but does not include necessary amendment to Internal Revenue Code subsection 6103(*l*) with conforming amendment to Internal Revenue Code subsection 6103(p)(4), IRS requests the agency develop a legislative proposal to do so. However, even in the absence of amendments to section 6103, constitutionally enacted legislation granting access to taxpayer data is still binding on IRS.

[99]Recipient agencies can only use the disclosed information for the purposes for which taxpayers consented to the disclosure. Additionally, recipient agencies cannot redisclose the information without permission from the taxpayer. 26 U.S.C. § 6103(c).

[100]42 U.S.C. §§ 1472, 1474, 1490a, 1490r.

[101]The Agriculture Improvement Act stated that the U.S. Department of Agriculture is granted the same access to information and subject to the same requirements applicable to the Department of Housing and Urban Development as provided in section 453 of the Social Security Act and subsection 6103(*l*)(7)(D)(ix) of the Internal Revenue Code. Pub. L. No. 115-334, § 6417, 132 Stat. 4490, 4763–4764 (2018).

disclosure for a nontax federal program. In instances where IRS has entered into an agreement to share information with other agencies for nontax programs, IRS officials told us they recently updated memorandums of understanding with receiving agencies to include section 6103 confidentiality requirements and data security safeguards.

IRS's actions, such as sharing data and codifying security requirements in a memorandum of understanding, are in line with Office of Management and Budget security and privacy guidance. This guidance states that agencies that share personally identifiable information with other agencies are to impose, where appropriate, conditions that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the information through written agreements. These agreements include contracts, data use agreements, information exchange agreements, and memorandums of understanding.[102]

According to its planning documentation, IRS is taking steps to address the gap in oversight of agencies receiving data via subsections Internal Revenue Code that are not subject to 6103(p)(4), but IRS may face challenges in doing so. IRS developed a strategic initiative that will conduct onsite inspections of federal agencies under these agreements when fully implemented. According to IRS draft planning documentation, beginning in fiscal year 2023, IRS plans to identify agencies receiving taxpayer information via certain subsections, including subsection 6103(c), and then determine an agency-specific course of action for IRS oversight. However, IRS's planning documentation notes that identifying all such data sharing agreements may be difficult because IRS does not have a good system that identifies all these initiatives and did not include a date for full implementation.

Data security could be further enhanced by updating Internal Revenue Code subsection 6103(p)(4) to include federal agencies with which IRS shares data via a taxpayer release under subsection 6103(c). This change would be in line with the additional safeguards the law requires for taxpayer information. It would also support IRS's ongoing efforts to

[102]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016), Appendix II - 7.

improve secure data and information sharing between national, local, and international stakeholders to collaborate on solving common problems.[103]

According to IRS officials, the agency has received numerous requests from other agencies to share taxpayer information as a result of recent legislation designed to reduce the economic effect of COVID-19, spur economic recovery, and reduce inflation. IRS officials said agencies would use the information to improve program administration and prevent fraud. However, Congress did not specifically provide for the use of the information in conforming legislative changes to Internal Revenue Code section 6103 for all of these programs. For example, according to IRS officials, a cross-functional agency team working on contact tracing for COVID-19 travel exposures wanted to use IRS's taxpayer information to help locate and contact individuals.

If the requirements of Internal Revenue Code subsection 6103(p)(4) were extended to agencies receiving taxpayer information via a signed taxpayer release under subsection 6103(c), then IRS would have the statutory authority to inspect these agencies' data safeguards and track their corrective actions.

Officials further explained that while IRS has not historically inspected of receiving agencies' safeguards for those agencies receiving data under subsection 6103(c), IRS officials assert the authority to review receiving agency safeguards in reliance on Internal Revenue Code subsection 6103(a)(1), among other authorities.

Extending subsection 6103(p)(4) safeguards and providing IRS with direct statutory authority to evaluate receiving agencies' data for taxpayer information IRS shares through subsection 6103(c) could help ensure those agencies protect taxpayer information with the same level of safeguards as other agencies that have been statutorily authorized to receive taxpayer information for specific programs.

[103]Internal Revenue Service, *Strategic Plan FY2022–2026*, Publication 3744 (July 2022).

Conclusions

Taxpayers' confidence and certainty in IRS's ability to protect their information is vital to the functioning of our tax system. To this end, IRS has increased safeguards to taxpayer information.

However, the security of taxpayer information could be strengthened through increased oversight of contractors who access taxpayer information and assist IRS in many of its activities and responsibilities. By doing more to make sure contractors complete required training, IRS could help ensure contractors have the knowledge to properly protect taxpayer information. This could also reduce IRS's burden of needing to disable and re-enable contractor access to its systems when contractors do not complete training on time. Further, providing training and guidance to the employees responsible for day-to-day oversight of contractors would give assurance that those employees will report incidents timely and accurately.

Improvements in IRS's monitoring of UNAX prevention efforts would also support the security of taxpayer information. Without maintaining a comprehensive inventory of systems, IRS cannot ensure it has implemented safeguards to protect taxpayer information on all of its systems. IRS may also be missing opportunities to identify business units with relatively high rates of UNAX cases out of the number of staff accessing taxpayer information that could benefit from training or targeted outreach. In a similar vein, IRS lacks insight into UNAX and unauthorized disclosure cases by IRS contractors. Assigning agency-wide responsibility for monitoring IRS contractor cases and ensuring there are quality data for this analysis are essential for IRS to determine if case amounts are changing and identify any trends across cases that could be used to target prevention efforts.

Finally, several information security weaknesses present risks to taxpayer data. IRS will have limited assurance that taxpayer information on certain IRS systems will be protected until the agency (1) develops appropriate security assessment and authorization documents for the system that tracks affluent taxpayers' risk of tax compliance; (2) implements procedures to determine when taxpayer information should no longer be stored in two research systems based on authorized retention periods; and (3) assesses the risk of its method for sharing data with external entities. Until IRS remediates IT control deficiencies, it will continue to

have limited information on risks to the security of taxpayer information and how to respond to those risks.

Congress could also help by providing IRS with the direct authority to inspect agencies' data safeguards in certain instances where IRS shares taxpayer information via a memorandum of understanding. These inspections could provide additional assurance that this information will be protected sufficiently.

Matter for Congressional Consideration

Congress should consider providing IRS with direct statutory authority to inspect receiving agencies' safeguards for taxpayer information shared under subsection 6103(c) of the Internal Revenue Code. (Matter for Consideration 1)

Recommendations

We are making the following 15 recommendations to IRS:

The Commissioner for Internal Revenue should officially assign the Human Capital Office responsibility for monitoring contractor training completion rates for courses related to protecting taxpayer information and ensure this role and responsibility is documented. (Recommendation 1)

The Commissioner for Internal Revenue should ensure that the Human Capital Office establish and document an agency-wide training completion goal for annual mandatory contractor training related to protecting taxpayer information. (Recommendation 2)

The Commissioner for Internal Revenue should ensure that the Human Capital Office monitor contractor training completion rates for courses related to protecting taxpayer information and take actions to ensure contractors complete training, such as sharing completion rates with contracting officer representatives (COR) and other appropriate offices. (Recommendation 3)

The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop guidance for CORs on the process of documenting and reporting

UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated. (Recommendation 4)

The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop training for CORs on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated. (Recommendation 5)

The Commissioner for Internal Revenue should ensure that the IT office, in collaboration with the Privacy, Governmental Liaison and Disclosure (PGLD) office, ensure that information is complete and accurate in the authoritative databases and other data sources that identify IRS systems that process or store taxpayer information. (Recommendation 6)

The Commissioner for Internal Revenue should ensure that the IT Cybersecurity office, in collaboration with PGLD, maintain a comprehensive inventory of IRS systems that process or store taxpayer information. (Recommendation 7)

The Commissioner for Internal Revenue should ensure that PGLD includes the number of IRS employees authorized to access taxpayer information in its UNAX case monitoring efforts. (Recommendation 8)

The Commissioner of Internal Revenue should direct the appropriate offices to ensure contractor data on UNAX and unauthorized disclosure cases are reliable and can be used to monitor case amounts and trends. (Recommendation 9)

The Commissioner for Internal Revenue should ensure that PGLD monitor contractor UNAX and unauthorized disclosure cases and trends and take action, as appropriate. (Recommendation 10)

The Commissioner for Internal Revenue should ensure that the IT Cybersecurity office ensure that the Large Business and International Division (LB&I) Pass-Through Entities office completes the inventory classification process for the system used for tracking affluent taxpayers' risk of tax noncompliance. (Recommendation 11)

The Commissioner for Internal Revenue should ensure that the LB&I Pass-Through Entities office develop key security assessment and authorization documentation, to include a system security plan and authorization to operate for the system used for tracking affluent

taxpayers' risk of tax noncompliance, as appropriate. (Recommendation 12)

The Commissioner for Internal Revenue should ensure that the Office of Research, Applied Analytics, and Statistics (RAAS) Data Management Division implement processes to determine when to delete taxpayer information residing in the Compliance Data Warehouse, if required, according to the approved Records Control Schedule. (Recommendation 13)

The Commissioner for Internal Revenue should ensure that the RAAS Data Management Division implement processes to determine when to delete or archive taxpayer information residing in the Link Analysis Tool, if required, according to the approved Records Control Schedule. (Recommendation 14)

The Commissioner for Internal Revenue should ensure that the Small Business/Self-Employment Division Collection office assess the risks of its method to transfer taxpayers' data electronically to private collection agencies, and take action, as appropriate. (Recommendation 15)

Agency Comments and Our Evaluation

We provided a draft of this report to IRS and the Treasury Inspector General for Tax Administration for review and comment. IRS provided written comments, which are summarized below and reproduced in appendix II. The Treasury Inspector General for Tax Administration said it did not have any comments on the report.

In its written comments, IRS agreed with 14 recommendations and disagreed with one. Specifically, IRS disagreed with the recommendation to implement processes to determine when to delete taxpayer information residing in CDW, if required, according to the approved Records Control Schedule (recommendation 13). In its letter, IRS requested that the recommendation be revised to read "delete or archive" to match the wording in recommendation 14.

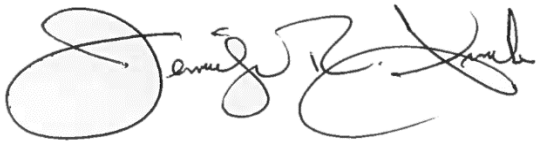
As we state in the report, IRS established a Records Control Schedule for CDW and the National Archives and Records Administration approved the schedule. The language in recommendation 13 is based on this approved schedule, which directs IRS to delete, not archive, system data 10 years after the end of the processing year or when no longer needed

for operational purposes. Therefore, we believe our recommendation remains warranted as originally drafted. The report further states that IRS is taking steps to update the CDW schedule to ensure it accurately reflects the business need for CDW data, which may include the option to delete or archive data. We will follow up with the agency on any changes to its Records Control Schedule and actions to implement this recommendation.

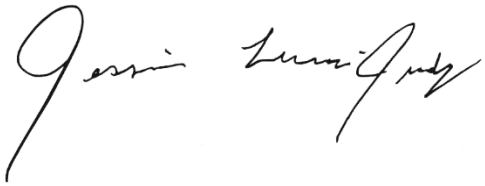
IRS also provided technical comments, which we incorporated where appropriate. We also edited the wording of recommendation 6 to clarify its intent.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 28 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Commissioner of Internal Revenue, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact us at (404) 679-1831 or FranksJ@gao.gov and (202) 512-6806 or LucasJudyJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity



Jessica Lucas-Judy
Director, Tax Issues
Strategic Issues

Appendix I: Objectives, Scope, and Methodology

This report evaluates the extent to which the Internal Revenue Service (IRS) is following its tax safeguards for protecting taxpayer information.

To address this objective, we analyzed the Treasury Inspector General for Tax Administration's (TIGTA) and our prior reports and recommendations related to cybersecurity and protecting taxpayer information, as well as IRS's actions to implement these recommendations. This enabled us to identify historical challenges IRS has faced protecting taxpayer information and steps IRS has taken to improve the security of taxpayer information.

We identified the implementation status of recommendations on TIGTA's website (https://www.tigta.gov/reports/list). According to a TIGTA official, recommendations are closed when planned corrective actions are taken. The official also stated that TIGTA neither validates the recommendation statuses nor requires validation before IRS closes recommendations. We did not assess the validity of the recommendation status information identified on TIGTA's website.

We reviewed our prior work related to protecting taxpayer information. We have performed a large body of work related to aspects of cybersecurity at IRS. For example, we annually audit IRS's financial statements to determine whether (1) the financial statements are presented fairly and (2) IRS management maintained effective internal control over financial reporting. This audit focuses on key systems relevant for storing, processing, and transmitting taxpayer and administrative financial information. It generally includes recommendations related to cybersecurity protections. We have also reviewed other aspects of cybersecurity at IRS, including the agency's response to breaches of personally identifiable information, the performance of IRS IT investments and risks of IRS legacy systems, taxpayer authentication, and IRS oversight of third-party cybersecurity practices. The following are descriptions of our work assessing aspects of cybersecurity at IRS:

- **Agency's response to breaches of personally identifiable information**: In this review, we (1) determined the extent to which selected agencies have developed and implemented policies and

procedures for responding to breaches involving personally identifiable information, and (2) assessed the role of the Department of Homeland Security in collecting information on breaches involving personally identifiable information and providing assistance to agencies. To do this, we analyzed data breach response plans and procedures at eight various-sized agencies, including IRS, and compared them to requirements in relevant laws and federal guidance and interviewed officials from those agencies and from the Department of Homeland Security.[1]

- **Performance of IRS IT investments and risks of IRS legacy systems**: We (1) evaluated the performance of selected IRS IT investments, (2) summarized any risks associated with selected legacy systems and evaluated the steps the agency has taken to manage such risks, and (3) determined the extent to which IRS has implemented key IT workforce planning practices. To meet these objectives, we analyzed planned versus actual performance information for nine selected investments for fiscal year 2016 and the first 2 quarters of fiscal year 2017—four in development and five in the operations and maintenance phase; identified risks facing three legacy investments and analyzed IRS's efforts to manage these risks against key practices; and analyzed IRS's IT workforce planning efforts against best practices.[2]
- **Taxpayer authentication**: We (1) described the taxpayer interactions that require authentication and IRS's methods; (2) assessed what IRS is doing to monitor and improve taxpayer authentication; and (3) determined what else, if anything, IRS can do to strengthen taxpayer authentication in the future. To meet these objectives, we reviewed IRS documents and data, evaluated IRS processes against relevant federal internal control standards and guidance, and interviewed IRS officials and state and industry representatives.[3]
- **IRS oversight of third-party cybersecurity practices**: 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

[1]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[2]GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

[3]GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts,* GAO-18-418 (Washington, D.C.: June 22, 2018).

reporting. We 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 National Institute of Standards and Technology (NIST) guidance and *Standards for Internal Control in the Federal Government*. We 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 A Framework for Managing Fraud Risk in Federal Programs. We also interviewed IRS and tax industry group officials.[4]

For reporting purposes, we categorized the security controls that we assessed into the five core security functions described in the NIST cybersecurity framework.[5]

- **Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[6]
- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

We discussed IRS's policies, procedures, and actions to protect taxpayer information and challenges to doing so with IRS officials in the Privacy, Disclosure and Governmental Liaison (PGLD) office—the office that

[4]GAO, *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices,* GAO-19-340 (Washington, D.C.: May 9, 2019).

[5]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

[6]According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an affect on organizational operations (including mission, capabilities, or reputation). National Institute of Standards and Technology, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Volume 2, Revision 1 (Gaithersburg, MD: December 2021), 62.

administers privacy, disclosure, identity assurance and records policies, procedures, and initiatives and coordinates those actions throughout IRS.

We also selected five IRS offices to understand how they protect taxpayer information and the challenges they face in doing so. Specifically, we selected

- Criminal Investigation;
- Large Business and International Division's (LB&I) Pass-Through Entities office;
- Office of Research, Applied Analytics, and Statistics (RAAS);
- Small Business/Self-Employed Division's Collection office; and
- Wage & Investment Division's Accounts Management office.

Our work based on these selected offices is nongeneralizable but gives us broad coverage to the different types of activities in which IRS engages—customer service (Accounts Management), collecting taxes owed (Collection), complex tax returns and issues and examination (LB&I Pass-Through Entities office), research and data management (RAAS), and law enforcement (Criminal Investigation).

We selected these offices by researching IRS's offices to determine which use taxpayer information in the course of their work and their different purposes. We selected offices to ensure they would reflect different types of activities so we would have a more comprehensive understanding of the different uses and safeguards of taxpayer information, such as including at least one office that

- is within IRS primary operating divisions;
- is not within IRS's primary operating divisions;
- has a high amount of willful unauthorized access, attempted access, or inspection of federal tax information (UNAX) violations;
- has a low amount of UNAX violations;
- has a field office presence; and
- works with contractors accessing taxpayer information.

We analyzed IRS documentation and data and interviewed IRS officials to identify the selected offices' safeguards for protecting taxpayer information. First, we interviewed IRS officials in the selected offices to understand their safeguards for protecting taxpayer information and the

process for reporting and investigating UNAX and unauthorized disclosure cases. We reviewed procedures from the IRS *Internal Revenue Manual* to determine if the selected offices' responses were in accordance with IRS policy. We also reviewed IRS's *Internal Controls Managerial Assessment* for fiscal year 2021, an annual self-assessment of internal controls where managers review the effectiveness of controls within their area of responsibility and verify that adequate management controls are in place and functioning effectively.

We also analyzed fiscal year 2021 data related to mandatory training for two groups: (1) all IRS employees, and (2) all IRS contractors in the five selected offices. These data come from the Department of the Treasury's Integrated Talent Management System, the system that IRS uses to track training completion data. We identified mandatory training related to protecting taxpayer information based on interviews with IRS officials in PGLD and the selected offices and our review of relevant *Internal Revenue Manual* sections.[7] Then we validated our list with PGLD.

As shown in table 7, we identified training courses related to protecting taxpayer information—four for IRS employees and five for IRS contractors. We then compared IRS employee training completion rates to the agency-wide goal of 97 percent completion. We analyzed IRS documentation and interviewed IRS officials to understand their efforts to monitor contractor training completion and their goals for contractor training completion rates. We compared IRS's efforts to monitor contractor training completion rates to internal controls related to monitoring in *Standards for Internal Control in the Federal Government*.[8]

Table 7: IRS Training Related to Protecting Taxpayer Information

Employee Type	Course	Description
IRS employees	UNAX Awareness	The objectives of this training are to identify which accesses are authorized, identify and report unauthorized accesses, identify inadvertent accesses and how to document these accesses, identify penalties for UNAX violations, and complete the required UNAX certification.

[7]Internal Revenue Service, *Internal Revenue Manual* § 10.5.1, Privacy Policy (July 26, 2021); *Internal Revenue Manual* § 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements (July 10, 2018); and *Internal Revenue Manual* § 11.3.1, Introduction to Disclosure (Mar. 13, 2018).

[8]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

Employee Type	Course	Description
IRS employees	Insider Threat Awareness	The training discusses the types of incidents that can occur and the reporting procedures, including the Situation Awareness Management Center, the central hub for reporting physical security incidents and emergencies that occur in the workplace.
IRS employees	IRS Annual Cybersecurity Awareness Training	This briefing covers security awareness, including protecting sensitive information, identifying phishing and spam emails, creating strong passwords to prevent data breaches, and proper disposal methods for equipment and documents, among other topics.
IRS employees	Privacy, Information Protection & Disclosure	This training explains why privacy is a vital component of the tax system; responsibilities related to protecting sensitive data and the privacy of employees and taxpayers; how to recognize common causes of data loss, unauthorized disclosures, and thefts; and how to report them.
IRS contractors	Introduction to UNAX	The objectives of this training are to identify which accesses are authorized, identify and report unauthorized accesses, identify inadvertent accesses and how to document these accesses, identify penalties for UNAX violations, and complete the required UNAX certification.
IRS contractors	Privacy, Information Protection & Disclosure	This training explains why privacy is a vital component of the tax system; responsibilities related to protecting sensitive data and the privacy of employees and taxpayers; how to recognize common causes of data loss, unauthorized disclosures, and thefts; and how to report them.
IRS contractors	Insider Threat Awareness	The training discusses the types of incidents that can occur and the reporting procedures, including the Situation Awareness Management Center, the central hub for reporting physical security incidents and emergencies that occur in the workplace.
IRS contractors	Inadvertent Sensitive Information Access	This training informs contractors of their responsibility to avoid inadvertent access to and disclosure of sensitive information. The training describes what information needs to be protected and why, how to identify inadvertent access situations, and how to protect sensitive information in response to an inadvertent access.
IRS contractors	IRS Annual Cybersecurity Awareness Training	This briefing covers security awareness, including protecting sensitive information, identifying phishing and spam emails, creating strong passwords to prevent data breaches, and proper disposal methods for equipment and documents, among other topics.

Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-23-105395

Note: UNAX is the willful unauthorized access, attempted access, or inspection of federal tax information. These courses were IRS's required courses for fiscal year 2021.

To assess the reliability of training data from the Integrated Talent Management System, we reviewed related documentation, interviewed knowledgeable officials, and conducted electronic data testing to identify missing values and obvious outliers and errors. We also compared our training completion rate calculations to IRS's internal documentation of such data to ensure consistency. We found the data to be sufficiently reliable for our purposes of reporting the number and percent of IRS

employees and contractors who completed annual training courses related to protecting federal taxpayer information for fiscal year 2021.

We analyzed IRS documentation and training materials and interviewed IRS contracting officer representatives (COR) to understand their roles and responsibilities overseeing contractors accessing taxpayer information. We reviewed IRS documentation on contractor security and privacy controls for handling and protecting information and training materials that instruct employees on how to report incidents.[9] We compared CORs' understanding of their roles overseeing contractors to IRS policies and procedures on CORs' responsibilities—including contractor security—outlined in these documents and training material.

We analyzed IRS documentation, interviewed IRS officials, and reviewed related TIGTA reports to evaluate the extent to which IRS monitors staff access to and disclosure of taxpayer information. Specifically, we analyzed IRS's system inventory that identified systems that store or process taxpayer information. We compared this inventory to systems the selected offices stated they use to store or process taxpayer information and identified systems that were missing from IRS's inventory. We reviewed IRS documentation and interviewed IRS officials to understand the missing systems and the reason for their omission.

We also reviewed IRS documentation and interviewed IRS officials to understand how IRS monitors, analyzes, and attempts to prevent UNAX cases. We compared that information to federal internal control standards related to quality information and monitoring; NIST standards and guidelines; Office of Management and Budget requirements for federal

[9]Internal Revenue Service, *Insider Threat Awareness Training* (2022); *Contractor Security & Privacy Controls: Handling and Protecting Information or Information Systems*, Publication 4812 (November 2021); and *Contracting Officer's Representative Handbook*, (Washington, D.C.: July 2020).

information, including the management of IT resources; IRS policies and guidance documents; and our guide to designing evaluations.[10]

We also analyzed IRS Human Capital Office data on UNAX and unauthorized disclosure cases from fiscal year 2017 through 2021 and related documentation and interviewed officials to determine how IRS monitors contractor UNAX and unauthorized disclosure cases. We found that IRS's e-Trak Report of Investigations Unit system contains information on contractor UNAX cases. However, we did not find it to be sufficiently reliable for the purpose of reporting on the number and characteristics of contractor UNAX cases.

We compared e-Trak Report of Investigations Unit data to other IRS misconduct case data, conducted electronic testing, and interviewed knowledgeable IRS officials. Specifically, we compared data from the e-Trak Report of Investigations Unit system on IRS employee UNAX cases to IRS's authoritative source on IRS employee misconduct cases (that includes IRS employee UNAX cases).[11] We followed up on data discrepancies with knowledgeable IRS officials to gain clarity. However, because the underlying records for this system are protected for taxpayer confidentiality, we could not review a sample of them to compare to IRS's e-Trak Report of Investigations Unit data to attempt to resolve data discrepancies. We discuss the data limitations we found in the report.

We further reviewed IRS documentation and interviewed IRS officials in various offices to understand the offices' roles in overseeing IRS contractors accessing taxpayer information. We then compared the available data on contractor UNAX cases and information on offices' roles in overseeing IRS contractors accessing taxpayer information to the

[10]GAO-14-704G; National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020); Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016); Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.1, UNAX Program Office Roles and Responsibilities (Mar. 8, 2023) and *Internal Revenue Manual* § 10.8.1.3.1.1.8.1, Unauthorized Access (UNAX) (May 9, 2019); and GAO, *Designing Evaluations: 2012 Revision (Supersedes PEMD-10.1.4)* GAO-12-208G (Washington, D.C.: Jan. 31, 2012).

[11]For our report analyzing the characteristics of IRS employee UNAX and unauthorized disclosure cases, IRS officials identified the Automated Labor and Employee Relations Tracking System as the most complete repository of UNAX case data at IRS. We found that data to be sufficiently reliable for reporting the number and characteristics of employee UNAX cases. For more information, see GAO-22-105872.

Internal Revenue Manual and internal controls related to monitoring and using quality information in the *Standards for Internal Control in the Federal Government*.[12]

We identified and tested selected management, operational, and technical controls (e.g., safeguards prescribed for a system to protect the confidentiality of the system and its information) at the agency-wide, system, and application levels, and observed controls in operation to evaluate IRS's information security controls for protecting taxpayer information.[13] We also conducted tests of controls to determine whether controls to help safeguard taxpayer information, and protect systems and application programs, were appropriately designed, implemented, and operating effectively. We also reviewed IRS documentation and interviewed IRS officials to understand how IRS designed and implemented those controls. We compared that information to requirements identified in NIST standards and guidelines, Office of Management and Budget guidance on *Managing Information as a Strategic Resource*, and IRS policies and guidance documents.[14]

[12]Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.1, IRP UNAX Program Team Roles and Responsibilities (July 10, 2018) and GAO-14-704G.

[13]Agency-wide level controls consist of the entity-wide processes that are focused on how the entity manages information security related to each type of control. For example, the agency may have broad entity-wide policies and procedures and implemented monitoring programs. Controls at the system level consist of processes for managing specific system resources related to either a general support system or major application. These controls are more specific than those at the entity-wide level and generally relate to a single type of technology. Controls at the application level consist of policies and procedures for controlling specific business processes.

[14]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020); *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18 (Gaithersburg, MD: February 2006); *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018); *Guide for Conducting Risk Assessments,* Special Publication 800-30, Revision 1 (Gaithersburg, MD: September 2012); Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016); and Internal Revenue Service, *Internal Revenue Manual* § 10.8.1, Information Technology (IT) Security, Policy and Guidance (Sept. 28, 2021); and *Federal Information Security Management Act (FISMA) Master Inventory Standard Operating Procedures,* Version 4.0 (Sept. 15, 2021).

We evaluated the controls for five selected IRS systems that process taxpayer information.[15] To select these systems, we identified systems our selected IRS offices accessed and excluded those that we had tested within the past 3 years as part of our annual audit of IRS's financial statements. We have ongoing work assessing the extent to which IRS appropriately designed and implemented technical controls to protect the confidentiality of federal tax information. We will publish this work in a subsequent report with limited distribution.

Finally, we also analyzed IRS documentation and relevant laws, and interviewed IRS officials. We analyzed the Taxpayer Browsing Protection Act and Internal Revenue Code section 6103 that set forth safeguards for taxpayer information and various laws authorizing other federal agencies to receive taxpayer information.[16] We analyzed agency documentation to understand how IRS shares information with other agencies and IRS's safeguards when doing so. We discussed IRS's policies, procedures, and actions to protect taxpayer information and challenges to doing so with IRS PGLD officials. We compared IRS's actions to protect taxpayer information and reported challenges to protecting taxpayer information to Office of Management and Budget guidance on *Managing Information as a Strategic Resource* and IRS's *Strategic Plan*.[17]

We conducted this performance audit from August 2021 to August 2023 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.

[15]Because we focused our evaluation on five systems, the results of our review of information security controls cannot be generalized to the entire IRS environment.

[16]Pub. L. No. 105-35, 111 Stat. 1104 (1997); 26 U.S.C. § 6103; for a law that authorized IRS to share taxpayer information, see, for example, Fostering Undergraduate Talent by Unlocking Resources for Education Act, Pub. L. No. 116-91, § 3(a), 133 Stat. 1189, 1189-1192 (2019).

[17]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016); Internal Revenue Service, *Strategic Plan FY2022–2026*, Publication 3744 (July 2022).

Appendix II: Internal Revenue Service Comments

DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 12, 2023

Ms. Jennifer R. Franks
Ms. Jessica K. Lucas-Judy
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Franks and Ms. Lucas-Judy:

I received the draft report entitled SECURITY OF TAXPAYER INFORMATION IRS Needs to Address Critical Safeguard Weaknesses (GAO-23-105395) and appreciate the opportunity to review and respond. The security of taxpayer information is one of the top priorities at the IRS. The IRS has instituted an extensive regimen of controls and monitoring to protect our networks and facilities. Additionally, the importance of security and privacy of sensitive information is reinforced to IRS employees through frequent communications and training.

Ensuring adequate controls are in place to protect federal tax information is a continuous process. As you note in your report, analyzing and improving access controls to sensitive information is on-going. The concept that employees and contractors only have access to the information that is needed to do their job is a foundational principle across the IRS. This principle is reinforced by the monitoring for Unauthorized Access of Taxpayer Accounts (UNAX) to identify situations where individuals access information that is not related to their assigned duties.

IRS has already implemented 83% of GAO's recommendations made since 2010, underscoring our commitment to these improvements. We appreciate the issues you raise; some recommendations are almost a decade old, and we will review the relevance of those items. It should be noted that there have been cases where IRS was required to prioritize recommendations due to lack of resources. Despite these challenges, IRS systems are secure and we are committed to improving our security posture going forward.

Again, thank you for providing the report and valuable feedback. We provided technical comments on the draft separately. If you have questions, please contact me, or a member of your staff may contact Kathleen Walters, chief privacy officer, at 202-317-4082.

Sincerely,

Jeffrey J. Tribiano

Digitally signed by Jeffrey J. Tribiano
Date: 2023.07.12 12:53:33 -04'00'

Jeffrey J. Tribiano
Deputy Commissioner for Operations Support

Enclosure

Enclosure

GAO Recommendations and IRS Responses to GAO Draft Report (GAO-23-105395)

Recommendation 1:
The Commissioner for Internal Revenue should officially assign the Human Capital Office responsibility for monitoring contractor training completion rates for courses related to protecting taxpayer information and ensure this role and responsibility is documented.

Comment:
IRS agrees with Recommendation 1, recognizing the need for the Human Capital Office to monitor contractor training completion rates.

Recommendation 2:
The Commissioner for Internal Revenue should ensure that the Human Capital Office establish and document an agency-wide training completion goal for annual mandatory contractor training related to protecting taxpayer information.

Comment:
IRS agrees with Recommendation 2, recognizing the need for the Human Capital Office to establish a training completion goal for contractors.

Recommendation 3:
The Commissioner for Internal Revenue should ensure that the Human Capital Office monitor contractor training completion rates for courses related to protecting taxpayer information and take actions to ensure contractors complete training, such as sharing completion rates with CORs and other appropriate offices.

Comment:
IRS agrees with Recommendation 3, recognizing the need for the Human Capital Office to monitor and share completion rates for contractors.

Recommendation 4:
The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop guidance for CORs on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

Comment:
IRS agrees with Recommendation 4. PGLD will coordinate the development of guidance for CORS on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

1

PGLD will coordinate with the Enterprise Contract Oversight Center to disseminate such guidance to the IRS COR community.

Recommendation 5:
The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop training for CORs on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

Comment:
IRS agrees with Recommendation 5. PGLD will coordinate the development of training for CORS on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated. PGLD will coordinate with the Enterprise Contract Oversight Center and with the Human Capital Office to deliver this training to the IRS COR community.

Recommendation 6:
The Commissioner for Internal Revenue should ensure that the IT organization, in collaboration with PGLD, ensures that information is complete and accurate in the authoritative databases and other data sources that identify IRS systems that process or store taxpayer information.

Comment:
IRS agrees with Recommendation 6. The Chief Information Officer, in collaboration with PGLD, will ensure that information is complete and accurate in the authoritative databases and other data sources that identify IRS systems that process or store taxpayer information.

Recommendation 7:
The Commissioner for Internal Revenue should ensure that the IT Cybersecurity Office, in collaboration with PGLD, maintain a comprehensive inventory of IRS systems that process or store taxpayer information.

Comment:
IRS agrees with Recommendation 7. The Chief Information Officer, in collaboration with PGLD, will maintain a comprehensive inventory of IRS systems that process or store taxpayer information.

Recommendation 8:
The Commissioner for Internal Revenue should ensure that PGLD includes the number of IRS employees authorized to access taxpayer information in its UNAX case monitoring efforts.

Comment:
IRS agrees with Recommendation 8. PGLD recognizes the need to track the number of employees authorized to access taxpayer information in monitoring for potential UNAX.

Recommendation 9:
The Commissioner for Internal Revenue should direct the appropriate offices to ensure contractor data on UNAX and unauthorized disclosure cases are reliable and can be used to monitor case amounts and trends.

Comment:
IRS agrees with Recommendation 9. PGLD recognizes the need for accurate information on potential contractor UNAX or unauthorized disclosures.

Recommendation 10:
The Commissioner for Internal Revenue should ensure that PGLD monitor contractor UNAX and unauthorized disclosure cases and trends and take appropriate action.

Comment:
IRS agrees with Recommendation 10. PGLD recognizes the need to monitor contractor UNAX and unauthorized disclosure cases and trends and take action.

Recommendation 11:
The Commissioner for Internal Revenue should ensure that the IT Cybersecurity Office ensure that LB&I Pass-Through Entities office completes the inventory classification process for the system used for tracking affluent taxpayers' risk of tax noncompliance.

Comment:
IRS agrees with Recommendation 11. The IT Cybersecurity Office recognizes the need to complete the inventory classification process.

Recommendation 12:
The Commissioner for Internal Revenue should ensure that the LB&I Pass-Through Entities office develop key security assessment and authorization documentation, to include a system security plan and authorization to operate for the system used for tracking affluent taxpayers' risk of tax noncompliance, as appropriate.

Comment:
IRS agrees with Recommendation 12. The LB&I Pass-Through Entities office recognizes the need to develop a system security plan.

Recommendation 13: The Commissioner for Internal Revenue should ensure that the RAAS Data Management Division implement processes to determine when to delete

taxpayer information residing in CDW, if required, according to the approved Records Control Schedule.

Comment:
IRS disagrees with Recommendation 13. RAAS requests that the recommendation be revised to read "delete or archive" to match the wording in recommendation 14.

Recommendation 14:
The Commissioner for Internal Revenue should ensure that the RAAS Data Management Division implement processes to determine when to delete or archive taxpayer information residing in YK1, if required, according to the approved Records Control Schedule.

Comment:
IRS agrees with Recommendation 14. The RAAS Data Management Division recognizes the need to implement processes to determine when to delete or archive taxpayer information.

Recommendation 15:
The Commissioner for Internal Revenue should ensure that the Small Business/Self-Employed Division Collection office assess the risks of its method to transfer taxpayers' data electronically to private collection agencies, and take action, as appropriate.

Comment:
IRS agrees with Recommendation 15. The Chief Information Officer will provide GAO with the risk assessment for the use of secure data transfer to electronically provide data to private collection agencies, and take action, if appropriate.

4

Accessible Text for Appendix II: Internal Revenue Service Comments

July 12, 2023

Ms. Jennifer R. Franks
Ms. Jessica K. Lucas-Judy
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Franks and Ms. Lucas-Judy:

I received the draft report entitled SECURITY OF TAXPAYER INFORMATION IRS Needs to Address Critical Safeguard Weaknesses (GAO-23-105395) and appreciate the opportunity to review and respond. The security of taxpayer information is one of the top priorities at the IRS. The IRS has instituted an extensive regimen of controls and monitoring to protect our networks and facilities. Additionally, the importance of security and privacy of sensitive information is reinforced to IRS employees through frequent communications and training.

Ensuring adequate controls are in place to protect federal tax information is a continuous process. As you note in your report, analyzing and improving access controls to sensitive information is on-going. The concept that employees and contractors only have access to the information that is needed to do their job is a foundational principle across the IRS. This principle is reinforced by the monitoring for Unauthorized Access of Taxpayer Accounts (UNAX) to identify situations where individuals access information that is not related to their assigned duties.

IRS has already implemented 83% of GAO's recommendations made since 2010, underscoring our commitment to these improvements. We appreciate the issues you raise; some recommendations are almost a decade old, and we will review the relevance of those items. It should be noted that there have been cases where IRS was required to prioritize recommendations due to lack of resources. Despite these challenges, IRS systems are secure and we are committed to improving our security posture going forward.

Again, thank you for providing the report and valuable feedback. We provided technical comments on the draft separately. If you have questions, please contact me, or a member of your staff may contact Kathleen Walters, chief privacy officer, at

202-317-4082.

Sincerely,

Jeffrey J. Tribiano
Deputy Commissioner for Operations Support

Enclosure

GAO Recommendations and IRS Responses to GAO Draft Report (GAO-23-105395)

Recommendation 1:

The Commissioner for Internal Revenue should officially assign the Human Capital Office responsibility for monitoring contractor training completion rates for courses related to protecting taxpayer information and ensure this role and responsibility is documented.

Comment:

IRS agrees with Recommendation 1, recognizing the need for the Human Capital Office to monitor contractor training completion rates.

Recommendation 2:

The Commissioner for Internal Revenue should ensure that the Human Capital Office establish and document an agency-wide training completion goal for annual mandatory contractor training related to protecting taxpayer information.

Comment:

IRS agrees with Recommendation 2, recognizing the need for the Human Capital Office to establish a training completion goal for contractors.

Recommendation 3:

The Commissioner for Internal Revenue should ensure that the Human Capital Office monitor contractor training completion rates for courses related to protecting taxpayer information and take actions to ensure contractors complete training, such as sharing completion rates with CORs and other appropriate offices.

Comment:

IRS agrees with Recommendation 3, recognizing the need for the Human Capital Office to monitor and share completion rates for contractors.

Recommendation 4:

The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop guidance for CORs on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

Comment:

IRS agrees with Recommendation 4. PGLD will coordinate the development of guidance for CORS on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

PGLD will coordinate with the Enterprise Contract Oversight Center to disseminate such guidance to the IRS COR community.

Recommendation 5:

The Commissioner for Internal Revenue should ensure that the Enterprise Contract Oversight Center and other appropriate offices develop training for CORs on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated.

Comment:

IRS agrees with Recommendation 5. PGLD will coordinate the development of training for CORS on the process of documenting and reporting UNAX and unauthorized disclosure incidents, including processes for cases that are substantiated. PGLD will coordinate with the Enterprise Contract Oversight Center and with the Human Capital Office to deliver this training to the IRS COR community.

Recommendation 6:

The Commissioner for Internal Revenue should ensure that the IT organization, in collaboration with PGLD, ensures that information is complete and accurate in the authoritative databases and other data sources that identify IRS systems that process or store taxpayer information.

Comment:

IRS agrees with Recommendation 6. The Chief Information Officer, in collaboration with PGLD, will ensure that information is complete and accurate in the authoritative databases and other data sources that identify IRS systems that process or store taxpayer information.

Recommendation 7:

The Commissioner for Internal Revenue should ensure that the IT Cybersecurity Office, in collaboration with PGLD, maintain a comprehensive inventory of IRS systems that process or store taxpayer information.

Comment:

IRS agrees with Recommendation 7. The Chief Information Officer, in collaboration with PGLD, will maintain a comprehensive inventory of IRS systems that process or store taxpayer information.

Recommendation 8:

The Commissioner for Internal Revenue should ensure that PGLD includes the number of IRS employees authorized to access taxpayer information in its UNAX case monitoring efforts.

Comment:

IRS agrees with Recommendation 8. PGLD recognizes the need to track the number of employees authorized to access taxpayer information in monitoring for potential UNAX.

Recommendation 9:

The Commissioner for Internal Revenue should direct the appropriate offices to ensure contractor data on UNAX and unauthorized disclosure cases are reliable and can be used to monitor case amounts and trends.

Comment:

IRS agrees with Recommendation 9. PGLD recognizes the need for accurate information on potential contractor UNAX or unauthorized disclosures.

Recommendation 10:

The Commissioner for Internal Revenue should ensure that PGLD monitor contractor UNAX and unauthorized disclosure cases and trends and take appropriate action.

Comment:

IRS agrees with Recommendation 10. PGLD recognizes the need to monitor contractor UNAX and unauthorized disclosure cases and trends and take action.

Recommendation 11:

The Commissioner for Internal Revenue should ensure that the IT Cybersecurity Office ensure that LB&I Pass-Through Entities office completes the inventory classification process for the system used for tracking affluent taxpayers' risk of tax noncompliance.

Comment:

IRS agrees with Recommendation 11. The IT Cybersecurity Office recognizes the need to complete the inventory classification process.

Recommendation 12:

The Commissioner for Internal Revenue should ensure that the LB&I Pass-Through Entities office develop key security assessment and authorization documentation, to include a system security plan and authorization to operate for the system used for tracking affluent taxpayers' risk of tax noncompliance, as appropriate.

Comment:

IRS agrees with Recommendation 12. The LB&I Pass-Through Entities office recognizes the need to develop a system security plan.

Recommendation 13: The Commissioner for Internal Revenue should ensure that the RAAS Data Management Division implement processes to determine when to delete taxpayer information residing in CDW, if required, according to the approved Records Control Schedule.

Comment:

IRS disagrees with Recommendation 13. RAAS requests that the recommendation be revised to read "delete or archive" to match the wording in recommendation 14.

Recommendation 14:

The Commissioner for Internal Revenue should ensure that the RAAS Data Management Division implement processes to determine when to delete or archive taxpayer information residing in YK1, if required, according to the approved Records Control Schedule.

Comment:

IRS agrees with Recommendation 14. The RAAS Data Management Division recognizes the need to implement processes to determine when to delete or archive taxpayer information.

Recommendation 15:

The Commissioner for Internal Revenue should ensure that the Small Business/Self-Employed Division Collection office assess the risks of its method to transfer taxpayers' data electronically to private collection agencies, and take action, as appropriate.

Comment:

IRS agrees with Recommendation 15. The Chief Information Officer will provide GAO with the risk assessment for the use of secure data transfer to electronically provide data to private collection agencies, and take action, if appropriate.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov

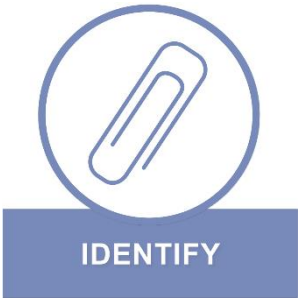
Jessica Lucas-Judy at (202) 512-6806 or LucasJudyJ@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Mark Canter (Assistant Director), Daniel Swartz (Assistant Director), Jason Vassilicos (Assistant Director), Dawn Bidne (Analyst-in-Charge), Kisa Bushyeager, Cassidy Cramton, Stephen Duraiswamy, Michele Fejfar, Mairé Gebhard, Robert Gebhart, Jackson Gode, Fatima Jahan, Krista Loose, Ahsan Nasar, Robert Robinson, Dawn Simpson, Andrew J. Stephens, and Rachel Stoiko made key contributions to this report.

Appendix IV: Additional Source Information for Icons

This appendix contains credit, copyright, and other source information for icons in this product when that information was not listed adjacent to the icon.



Source: GAO presentation of National Institute of Standards and Technology Cybersecurity Framework; bsd studio/stock.adoble.com.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548