

GAO Highlights

Highlights of [GAO-23-105395](#), a report to congressional requesters

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.

August 2023


SECURITY OF TAXPAYER INFORMATION

IRS Needs to Address Critical Safeguard Weaknesses

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

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.

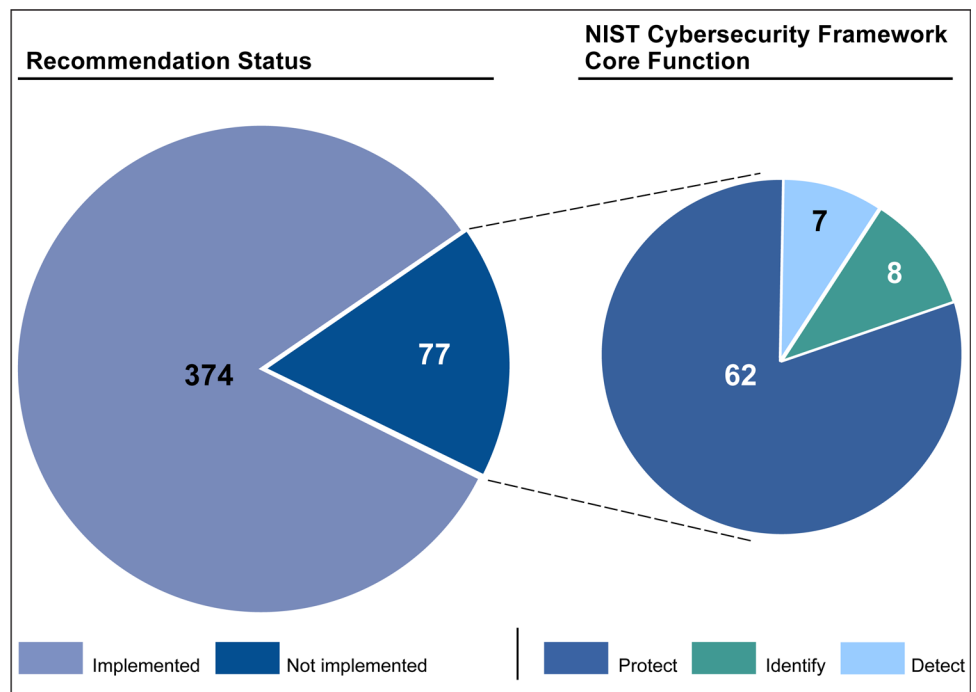
View [GAO-23-105395](#). For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov or Jessica Lucas-Judy at (202) 512-6806 or LucasJudyJ@gao.gov.

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

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.