TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Efforts to Oversee State Agency Access to Federal Tax Information Were Generally Successful; However, Some Improvements Are Needed

August 23, 2024

Report Number: 2024-100-041

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Efforts to Oversee State Agency Access to Federal Tax Information Were Generally Successful; However, Some Improvements Are Needed

Final Audit Report issued on August 23, 2024 **Report Number 2024-100-041**

Why TIGTA Did This Audit

Internal Revenue Code § 6103 permits the disclosure of Federal Tax Information (FTI) to State, Territory, and local agencies. Congress balanced this disclosure authority with requirements designed to safeguard FTI against misuse and unauthorized disclosure as well as penalties for those who violate the law.

This audit was initiated to determine whether the Office of Safeguards provides adequate oversight of State agencies receiving FTI.

Impact on Tax Administration

To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the IRS is protected against unauthorized use, inspection, or disclosure.

The Office of Safeguards verifies compliance with safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of FTI held by over 250 State, Territory, and local agencies.

In addition, the Office of Safeguards is responsible for producing and revising Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*, which provides guidance to ensure that the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or subcontractors adequately protect the confidentiality of FTI.

What TIGTA Found

The Office of Safeguards has developed extensive internal and external training resources and maintained a safeguard review schedule that has led to the completion of safeguard reviews for 98 percent of active State agencies in the past three years. Although the Office of Safeguards has established due dates for annual Safeguard Security Reports and semiannual Corrective Action Plans, State agencies did not always provide that information timely. For example, TIGTA determined that 135 (54 percent) of the 251 Safeguard Security Reports required to be submitted by State agencies in Calendar Year 2022 were timely, 104 (41 percent) were received late, and 12 (5 percent) were never received.

In addition, 15 (23 percent) of the 66 data incidents reported by State agencies in Calendar Year 2022 were not reported to the Office of Safeguards within 24 hours of identification, as required. The remaining 51 (77 percent) were timely reported. The most common data incidents included sending FTI to the wrong taxpayer, access by an unauthorized individual, or e-mailing FTI either internally or externally. Further, 19 (30 percent) of 63 State agencies did not provide a mitigation plan for critical findings identified during a Calendar Year 2022 safeguard review within seven days of the closing conference, as required. This included two agencies that did not provide a mitigation plan at all. While 41 (65 percent) State agencies timely provided their critical finding mitigation plans, TIGTA was unable to determine the mitigation plan receipt date for three (5 percent) agency responses because the date was not included in eCase.

What TIGTA Recommended

TIGTA recommended that the Chief Privacy Officer: 1) subsequently remind agencies with late-filed Safeguard Security Reports or Corrective Action Plans of best practices at least 60 days prior to their next scheduled filing due date; 2) offer standardized training to any new Head of Agency on the safeguard review process; 3) update policies to require follow-up with State agencies concerning any unsubmitted mitigation plans after their mitigation plan due dates have passed; 4) develop procedures to ensure that accurate and complete information is included in safeguard review documentation and eCase; and 5) send an annual reminder to all State agencies to notify staff of their responsibility to report data incidents within 24 hours of identification. The IRS agreed with all five recommendations and has developed corrective actions for each.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

August 23, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Efforts to Oversee State Agency Access to Federal Tax Information Were Generally Successful; However, Some Improvements Are Needed (Audit No.: 202310007)

This report presents the results of our review to determine whether the Office of Safeguards provides adequate oversight of State agencies receiving Federal Tax Information. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix II. If you have any questions, please contact me or Bryce Kisler, Assistant Inspector General for Audit (Management Services and Exempt Organizations).

Table of Contents

Background

The Internal Revenue Service (IRS) provides Federal Tax Information (FTI) to over 250 State, Territory, and local agencies (hereafter referred to as State agencies).[1] This exchange of confidential tax information is intended to improve tax administration by reducing duplicate government resource expenditures and increasing taxpayer compliance. Congress has recognized the importance of this exchange program under Internal Revenue Code (I.R.C.) § 6103 by permitting the disclosure of FTI to State agencies. Congress balanced this disclosure authority with requirements designed to safeguard FTI against misuse and unauthorized disclosure.[2] The I.R.C. defines and protects the confidential relationship between the taxpayer and the IRS and makes it a crime to violate this confidence.[3] To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the IRS is protected against unauthorized use, inspection, or disclosure.

The Office of Safeguards

The Privacy, Governmental Liaison, and Disclosure function's Office of Safeguards is responsible for ensuring that any FTI made available to State agencies and their contractors is adequately protected. The Office of Safeguards verifies compliance with I.R.C. § 6103(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of FTI held by external government agencies. The Office of Safeguards is also responsible for producing and revising Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*, which provides guidance to ensure that the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or subcontractors adequately protect the confidentiality of FTI. In accordance with I.R.C. § 6103(p)(5), the IRS is required to submit an annual report to Congress regarding the procedures and safeguards established by the various State agencies and their respective contractors that receive FTI as well as identifying any deficiencies.

Safeguard Security Reports (SSR)

As a condition of receiving FTI, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. State agencies must implement certain safeguards to prevent unauthorized access and use. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected. An agency must ensure that its safeguards will be ready for immediate

[1] FTI consists of Federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements, including IRS oversight.

[2] I.R.C. § 6103(p)(4) requires that agencies receiving tax returns and return information provide adequate safeguards to protect the confidentiality of the tax returns and return information to the satisfaction of the Secretary of the Treasury.

[3] I.R.C. § 7213 prescribes criminal penalties, making it a felony offense for Federal and State employees and others to illegally disclose FTI. I.R.C. § 7213A makes the unauthorized inspection of FTI a misdemeanor, punishable by fines, imprisonment, or both.

implementation upon receipt of any FTI. I.R.C. § 6103(p)(4)(E) requires State agencies to file a SSR that describes the procedures established and used by the agency for ensuring the confidentiality of information received from the IRS. An initial SSR must be submitted for the Office of Safeguards' approval at least 90 days prior to the agency receiving FTI. The agency's SSR must describe the purpose(s) for which FTI is collected, used, maintained, and shared. State agencies are then required to submit an annual SSR encompassing any changes that impact the protection of FTI by the due date assigned for that State. The SSR and any supplemental information is documented and maintained in eCase.[4] A total of 251 State agencies were required to submit the SSRs in Calendar Year (CY) 2022.

Safeguard reviews

A safeguard review is an evaluation of the use of FTI and the measures employed by the receiving agency and its agents (where authorized) to protect the data.[5] Safeguard reviews are conducted to determine the adequacy of safeguards and focus on the following:

State agencies are typically reviewed once every three years, and the Office of Safeguards schedules review dates by State. This allows all agencies within a State to participate in a safeguard review around the same time. While reviews are typically scheduled on a three-year basis, Office of Safeguards personnel did indicate that an agency may be deferred due to various scheduling factors at the request of its Head of Agency (HOA). However, the Office of Safeguards also selects State agencies for out-of-cycle reviews outside the three-year period, using a risk management approach to identify agencies with vulnerabilities in their processes for protecting FTI.[6]

Office of Safeguards personnel must complete the Preliminary Findings Report (PFR) during the safeguard review and provide the State agencies an overview of the findings that require correction to improve the safeguarding of FTI. For each safeguard review finding, the evaluated risk of potential loss, breach, or misuse of FTI establishes the recommended time frame for resolution. Findings are assigned a risk level of critical, significant, moderate, or limited, with

[4] A cloud-based case management application tailored for the Office of Safeguards.

[5] The review includes an in-person evaluation of physical security controls and a remote evaluation of computer security controls.

[6] The Office of Safeguards considers unresolved physical and computer security findings from an agency's latest review as well as an agency's efforts to comply with safeguard reporting requirements.

critical being the highest risk. State agencies are required to complete corrective actions related to these findings within three months to a year depending on the risk level. For critical findings, the agency must also submit a mitigation plan to the Office of Safeguards within seven days of the closing conference. Figure 1 describes the finding risk categories.

Figure 1: Safeguard Review Finding Categories

Risk Category	Definition	Resolution Time Frame
Critical	The potential impact is **Critical** if the vulnerability has an immediate adverse effect on the confidentiality and integrity of FTI.	3 months from the date of the review closing conference.
Significant	The potential impact is **Significant** if the vulnerability could be expected to have a severe or an imminent adverse effect on the ability to maintain the confidentiality and integrity of FTI.	6 months from the date of the review closing conference.
Moderate	The potential impact is **Moderate** if the vulnerability could be expected to have a demonstratable adverse effect on the ability to maintain the confidentiality and integrity of FTI.	9 months from the date of the review closing conference.
Limited	The potential impact is **Limited** if the vulnerability could be expected to have a low or minimal adverse effect on the ability to maintain the confidentiality and integrity of FTI.	12 months from the date of the review closing conference.

Source: Internal Revenue Manual (IRM) 11.3.36, Disclosure of Official Information, Safeguards Review Program (July 21, 2015) and Publication 1075.

Each safeguard review is followed by a closing conference, where the PFR is issued to the State agency. A Safeguard Review Report (SRR) and Corrective Action Plan (CAP) are then issued to the State agency by the Office of Safeguards within 45 days of the closing conference to finalize the safeguard review findings. The SRR serves as a record of the IRS's evaluation of an agency's compliance with the safeguard requirements for the protection of FTI. The CAP is a report containing the findings, recommended corrective actions, and targeted implementation dates for each weakness identified during a safeguard review. State agencies use the CAP to provide details on their planned and completed actions to address each finding. State agencies are required to submit their CAP updates semiannually and as an attachment to their SSRs. Figure 2 describes the safeguard review process.

Figure 2: Safeguard Review Process

Source: IRM 11.3.36, Publication 1075, and training materials.

Results of Review

The IRS's efforts to oversee State agencies' access to FTI were generally successful. The Office of Safeguards has developed extensive internal and external training, and guidance outlining the process State agencies must follow to safeguard FTI. In addition, the Office of Safeguards has developed and maintained a safeguard review schedule that led to completing safeguard reviews for 98 percent of active State agencies in the past three years.[7] The Office of Safeguards has also established comprehensive guidance and policies to ensure that consistent risk levels are assigned to safeguard review findings of the same type and that its annual report to Congress was submitted timely. However, some State agencies did not comply with safeguard requirements or provide required information to the Office of Safeguards timely.

Some State Agencies Did Not Comply With Federal Tax Information Safeguard Requirements

Publication 1075 outlines the safeguard requirements for State agencies that have access to FTI. This includes annual reporting requirements via the SSR, real-time reporting of data incidents, and semiannual reporting of corrective actions related to findings from a safeguard review. Although the Office of Safeguards has established due dates for annual SSRs and semiannual CAP update reports, State agencies do not always provide that information timely. In addition, State agencies do not always report data incidents to the Office of Safeguards within 24 hours of identification or provide mitigation plans for critical findings identified during a safeguard

[7] The remaining safeguard reviews have been scheduled.

review within seven days of the closing conference, as required. While most State agencies complied with these requirements, the Office of Safeguards needs to increase monitoring and outreach for noncompliant agencies and ensure that they are held accountable when they do not comply.

Some State agencies did not timely submit the SSRs

We determined that 135 (54 percent) of the 251 SSRs required to be submitted by State agencies in CY 2022 were timely, 104 (41 percent) were received late, and 12 (5 percent) were never provided. State agencies provided the 104 late SSRs up to 392 days after the due date with 60 SSRs provided within 30 days of the due date, 21 SSRs provided within 31 to 60 days of the due date, and the remaining 23 SSRs provided more than 60 days late.

The SSR is the primary method for State agencies to report to the Office of Safeguards on the processes and procedures they have in place to protect FTI. State agencies have an annual requirement to submit the SSRs after their initial receipt of FTI. The purpose of the SSR is for agencies to document the implementation of security and privacy controls that affect the protection of FTI. Each SSR submission must include a description of the updates or changes that have occurred during the reporting period. SSR submissions must include a signed certification letter from the HOA or their designee with the agencies being required to use the official templates provided by the Office of Safeguards. Figure 3 shows the list of SSR submission deadlines by State or Territory.

Figure 3: SSR Submission Deadlines by State or Territory

Partner Agency State or Territory	Reporting Period	Due Date
Alabama, Alaska, American Samoa, Arizona, Arkansas, California	February 1 – January 31	February 28
Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Northern Mariana Islands	March 1 – February 28	March 31
Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas	April 1 – March 31	April 30
Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan	May 1 – April 30	May 31
Minnesota, Mississippi, Missouri, Montana, Nebraska	June 1 – May 31	June 30
Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina	July 1 – June 30	July 31
North Dakota, Ohio, Oklahoma, Oregon	August 1 – July 31	August 31
Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee	September 1 – August 31	September 30
Texas, Utah, Vermont, Virgin Islands, Virginia, Washington	October 1 – September 30	October 31
West Virginia, Wisconsin, Wyoming	November 1 – October 31	November 30

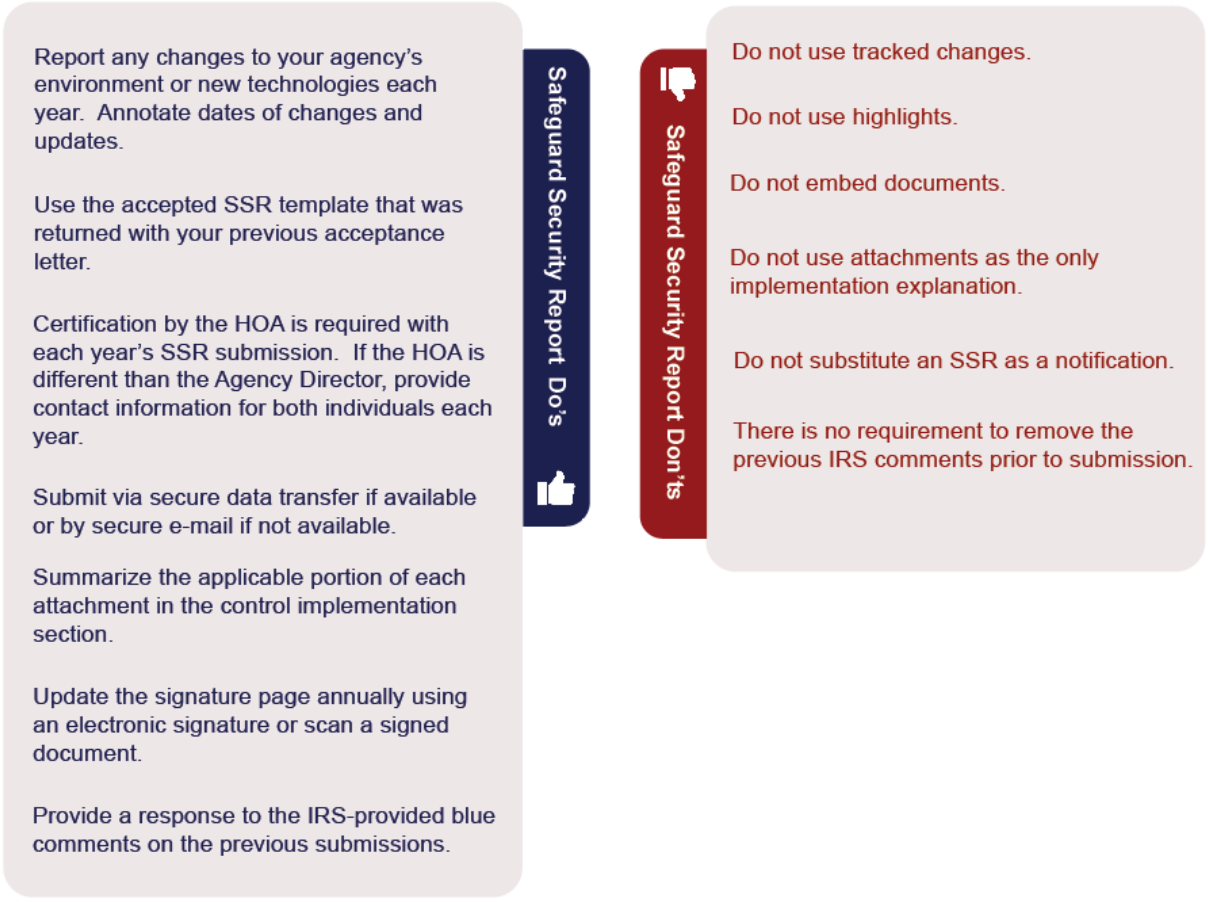
Source: Publication 1075.

When extenuating circumstances exist, State agencies may request an SSR extension in 30-day increments, with a maximum of 60 days. Extension requests must be submitted no later than 30 days prior to the scheduled SSR due date. Of the 104 late SSRs in CY 2022, 25 would have been considered timely, but had inadequacies that the State agencies were required to correct. Examples of common SSR inadequacies include a missing certification from the HOA, documentation submissions in the wrong format, and submissions missing required information. The remaining 79 were not originally submitted until after the due date.

I.R.C. § 6103(p)(4) provides that the IRS may take necessary actions to ensure that State agencies are meeting their safeguard requirements. Such actions may include refusing to disclose returns or return information until it is determined that the safeguard requirements have been or will be met. Per the IRM, enforcement related to the submission of the SSRs may occur if an SSR has not been filed for two consecutive years. In this case, the HOA would be notified that the IRS intends to discontinue the disclosure of FTI to their agency. Of the 12 agencies that did not submit a CY 2022 SSR, all but three submitted an SSR in CY 2021. Office of Safeguards management did not pursue enforcement actions against the three agencies because two no longer receive FTI, and the active agency made attempts to submit its CY 2022 SSR, but the IRS was unable to open the attachments. The agency successfully submitted its CY 2023 SSR in January 2024.

According to Office of Safeguards management, there are no IRM or standard operating procedure directions specifying that Office of Safeguards personnel should send individual reminders to agencies in advance of their annual SSR due date. However, the Office of Safeguards does hold quarterly "office hour" calls to answer agency questions and has posted SSR best practices on IRS.gov, as shown in Figure 4.

Figure 4: Office of Safeguards SSR Best Practices



Source: The Safeguards Program page on IRS.gov (June 2024).

A late or missing SSR delays the Office of Safeguards' ability to review and evaluate changes to an agency's FTI safeguards. It also delays the Office of Safeguards' efforts to confirm that issues identified in the previous year's SSR have been addressed.

Some State agencies did not timely submit CAP updates

We reviewed documentation in eCase for a judgmental sample of 14 out of the 87 safeguard reviews completed in CY 2022 and determined that six (43 percent) of the 14 required CAPs were received timely, seven (50 percent) were received late, and one (7 percent) CAP was not submitted at all.[8] Of the seven late CAPs, three were submitted to the Office of Safeguards one to 10 days late, one was over 30 days late, and three were over 100 days late. Office of Safeguards management issued a late submission notice in August 2023 to the one State agency that did not submit its CAP update following its CY 2022 safeguard review, but did not pursue any additional enforcement actions because the agency made attempts to submit its CAP. The agency successfully submitted a CAP update in April 2024.

[8] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

State agencies are required to update and submit their CAP updates semiannually to document all corrective actions, planned or taken, in response to findings identified during a safeguard review. Figure 5 provides a list of CAP submission due dates by State or Territory.

Figure 5: CAP Submission Deadlines by State or Territory

Partner Agency State or Territory	CAP With SSR Submission Date	CAP Only Submission Date
Alabama, Alaska, American Samoa, Arizona, Arkansas, California	February 28	August 31
Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Northern Mariana Islands	March 31	September 30
Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas	April 30	October 31
Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan	May 31	November 30
Minnesota, Mississippi, Missouri, Montana, Nebraska	June 30	December 31
Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina	July 31	January 31
North Dakota, Ohio, Oklahoma, Oregon	August 31	February 28
Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee	September 30	March 31
Texas, Utah, Vermont, Virgin Islands, Virginia, Washington	October 31	April 30
West Virginia, Wisconsin, Wyoming	November 30	May 31

Source: Publication 1075.

Each State agency's CAP details the actions completed to address findings identified during a safeguard review or planned actions with a scheduled implementation date. This includes the requirement that agencies provide supporting documentation to the Office of Safeguards for validation prior to the closure of critical and significant findings. If an agency does not submit a CAP update for multiple periods in a row, the IRS can pursue enforcement actions, which may include the suspension or termination of FTI access.

We reviewed CAP documentation for the judgmental sample of 14 out of the 87 safeguard reviews completed in CY 2022 and noted that the Office of Safeguards identified deadlines for resolution based on the risks associated with each finding and provided comments to address the issues in a timely fashion. In addition, the Office of Safeguards considered supporting documentation from State agencies before closing critical findings and identified the type of supporting documentation required to close the open findings.

While Office of Safeguards management could not determine the actual reasons why State agencies sent CAP updates late, they noted that delays may have been due to State agency personnel or point of contact changes, such as the HOA. These new personnel may not be as familiar with the CAP process. Office of Safeguards management also indicated that State agencies may not submit a CAP update timely because they are waiting on supporting departments, such as an agency's Information Technology organization, to finalize a solution. In addition, the Office of Safeguards does not provide standardized training to State agency personnel, other than quarterly "office hour" calls. Office of Safeguards management also

confirmed that there is no requirement to send reminders to State agencies in advance of their CAP due dates.

The Office of Safeguards typically provides both positive and negative feedback to State agencies on all planned or completed corrective actions. Positive feedback conveys that the Office of Safeguards accepts the agency's response and confirms the finding is closed when the action is completed. Negative feedback typically includes a statement that the agency's response is not accepted and a description of what is required for the corrective action to be adequate. For all four agencies that submitted their CAPs over 30 days late, the IRS provided negative feedback on multiple findings. Late CAP updates delay the Office of Safeguards ability to provide this feedback. In addition, findings identified during a safeguard review may remain uncorrected, which would continue to put FTI at risk. If State agencies continually send in late CAP updates, the Office of Safeguards should consider enforcement actions.

Some mitigation plans to address critical safeguard review findings were untimely and were not consistently documented

We reviewed documentation in eCase for 63 State agencies with critical findings identified during a CY 2022 safeguard review and determined that 41 (65 percent) of 63 State agencies provided a mitigation plan to the Office of Safeguards within seven days of the closing conference, as required. Of the 19 (30 percent) mitigation plans that were not provided timely, five were submitted within 10 days of the due date and 12 were submitted within 11 to 21 days of the due date. The remaining two agencies never provided a mitigation plan to the Office of Safeguards.[9] In addition, we were unable to determine the mitigation plan receipt date for three (5 percent) of 63 agency responses because the date was not included in eCase.

Publication 1075 requires a State agency to submit a mitigation plan to the Office of Safeguards within seven days of the closing conference to address any critical findings identified during a safeguard review. This plan allows the Office of Safeguards to assess the agency's strategy for correcting identified deficiencies. However, safeguard review policies do not require follow-up when mitigation plans are submitted late. By reviewing case notes and safeguard review documentation in eCase, we determined that the Office of Safeguards does not always follow up with the State agency once this due date has passed.[10] In addition, the Office of Safeguards does not consistently document the mitigation plan receipt date in eCase. For the two agencies that did not provide a mitigation plan at all, Office of Safeguards management acknowledged that the finding risk category was inaccurately recorded on the PFR, and in eCase, so the agencies were unaware that they had critical findings at the time of the closing conference and were never asked for a mitigation plan. The risk category was also incorrectly recorded on the final SRR. Of the two agencies, one did not implement corrective actions for the associated critical finding within three months, as required.

When a State agency provides a late mitigation plan to the Office of Safeguards, or no plan at all, the Office of Safeguards is unable to assess the agency's planned mitigation strategy or document completed updates to safeguard procedures. This could result in a critical finding remaining unresolved, which has the potential to put FTI at risk. When the Office of Safeguards

[9] All critical findings for these two agencies are closed.

[10] The notes tab is eCase is used to view, add, and edit case updates, cases notes, and relevant correspondence.

does not assign the correct risk level to a finding in the PFR and eCase, a State agency may not be aware that a mitigation plan is required.

State agencies did not timely report all data incidents

Of the 66 data incidents reported to the Office of Safeguards by State agencies in CY 2022, 51 (77 percent) were reported within 24 hours of the incident, as required.[11] Of the 15 (23 percent) incidents that were not reported within 24 hours, six were reported one day late, four were reported two to four days late, and the remaining five were 13 to 42 days late. The most common data incidents included sending FTI to the wrong taxpayer, access by an unauthorized individual, or e--mailing FTI either internally or externally.

77 percent of data incidents were reported within 24 hours, as required.

23 percent ranged from one to 42 days late.

Publication 1075 outlines reporting requirements when a Federal employee, a State employee, or any other person discovers a possible improper inspection or disclosure of FTI, including data breaches and data incidents.[12] The individual making the observation or receiving information must concurrently notify the Office of Safeguards and the Treasury Inspector General for Tax Administration's Office of Investigations immediately, but no later than 24 hours after identification of a possible issue involving FTI. In August 2023, the Office of Safeguards issued interim guidance in coordination with the Treasury Inspector General for Tax Administration's Office of Investigations to inform State agencies that going forward, improper inspections or disclosures will only need to be reported to the Office of Safeguards.[13]

Office of Safeguards management stated that there is no requirement for the IRS to send annual reminders to State agencies regarding their responsibility to report data incidents. Publication 1075 requires that agencies complete awareness training annually, which should include data incident response and reporting requirements, and the criminal and civil penalties associated with unauthorized access and disclosure of FTI. However, for one late incident report, the State agency indicated that they failed to communicate to staff members that external notifications were required for the incident type.[14] An untimely or unreported data incident could put FTI at increased risk and delay the Office of Safeguards' ability to ensure that the issue has been corrected.

[11] A data incident is an occurrence that: 1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system or 2) constitutes a violation or an imminent threat of a violation of law, security policies, security procedures or acceptable use policies. Incidental and inadvertent accesses are considered data incidents.

[12] A data breach is a type of incident involving a loss, theft, or inadvertent disclosure of FTI.

[13] The Office of Safeguards plans to include this change in the next update to Publication 1075.

[14] This data incident involved the loss of an agency issued cell phone.

The Chief Privacy Officer should:

Recommendation 1: Subsequently remind agencies with late-filed SSRs or CAPs of best practices at least 60 days prior to their next scheduled filing due date, and that they may request a filing extension at least 30 days before their scheduled due date if extenuating circumstances exist.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Safeguards will e-mail a reminder to the points of contact for agencies with late-filed SSRs or CAPs at least 60 days prior to their next scheduled filing due date. The Office of Safeguards will issue guidance to document this ongoing requirement.

Recommendation 2: Offer standardized training to any new HOA on the safeguard review process and best practices for submitting agency documentation.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Safeguards will e-mail a Security and Privacy Alert to agencies publicizing the availability of standardized training for new HOAs on the safeguard review process and best practices for submitting agency documentation to be delivered using a virtual meeting presentation to allow for a live question and answer exchange.

Recommendation 3: Update policies to require follow-up with State agencies concerning any unsubmitted mitigation plans after their mitigation plan due dates have passed.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Safeguards will issue guidance to document the requirement to follow up with State agencies to secure mitigation plans not submitted by the established due date.

Recommendation 4: Develop procedures to ensure that finding information is accurately documented in the PFR, the SRR, and eCase as well as that case updates, case notes, relevant correspondence, and mitigation plan receipt dates are accurately documented in eCase.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Safeguards will issue guidance on the procedures to follow to validate the accuracy of findings documented in the PFR, the SRR, and eCase, and to validate the accuracy of eCase updates, case notes, relevant correspondence, and mitigation plan receipt dates.

Recommendation 5: Send an annual reminder to all State agencies to notify staff of their responsibility to report data incidents within 24 hours of identification.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Safeguards will e-mail a reminder to the points of contact for agencies to notify staff of their responsibility to report data incidents within 24 hours of identification. The Office of Safeguards will issue guidance to document this ongoing requirement.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the Office of Safeguards provides adequate oversight of State agencies receiving FTI. To accomplish our objective, we:

- Obtained an understanding of the policies, procedures, and controls used by the Office of Safeguards to oversee the State agencies that receive FTI by reviewing documentation and interviewing Office of Safeguards personnel.
- Determined whether the Office of Safeguards receives and reviews the SSRs for State agencies requesting access to FTI in accordance with established policies and procedures.
- Determined whether the Office of Safeguards is complying with established policies and procedures pertaining to safeguard reviews by assessing the safeguard review schedule, consistency of assigned risk levels for review findings, and timeliness of SRR and CAP issuance.
- Reviewed documentation for a judgmental sample of 14 out of the 87 safeguard reviews completed in CY 2022 based on the volume and quality of information contained in each case.[1] We selected the safeguard reviews based on the number of critical findings and non-information technology findings identified in each review.

Performance of This Review

This review was performed with information obtained from the Privacy, Governmental Liaison, and Disclosure function's Office of Safeguards in Washington, D.C., and Topeka, Kansas, during the period June 2023 through May 2024. We conducted this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Bryce Kisler, Assistant Inspector General for Audit (Management Services and Exempt Organizations); Glen Rhoades, Director; Melinda Dowdy, Audit Manager; Zachary Orrico, Lead Auditor; and Tak Kin Andy Lee, Auditor.

Data Validation Methodology

We performed tests to assess the reliability of data from eCase. We evaluated the data by 1) obtaining direct access to the systems, 2) performing electronic testing of required data elements, 3) reviewing existing information about the data and the system that produced them, and 4) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Publication 1075, the IRM, and the Office of Safeguards policies, procedures, and practices for providing oversight to State agencies that receive FTI in accordance with I.R.C. § 6103(p)(4). We evaluated these controls by reviewing source documents in eCase, interviewing Office of Safeguards management, and attending a safeguard review.

Appendix II

Management's Response to the Draft Report

CHIEF PRIVACY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 22, 2024

MEMORANDUM FOR DANNY VERNEUILLE
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Phyllis T. Grimes
Acting Chief Privacy Officer

Phyllis T. Grimes Digitally signed by Phyllis T. Grimes Date: 2024.07.23 12:14:56 -04'00'

SUBJECT: Draft Audit Report - Efforts to Oversee State Agency Access to Federal Tax Information Were Generally Successful; However, Some Improvements Are Needed (Audit # 202310007)

Thank you for the opportunity to respond to the above referenced draft audit report. The IRS remains committed to oversight of the security of federal tax information in the possession of state agencies. We appreciate your recognition of the positive steps taken by the IRS to operate an effective Safeguards program.

We agree with the recommendations. We value the Treasury Inspector General for Tax Administration identifying the need to remind state agencies of their obligations to submit required reports timely; to offer training to new state agency heads; to take follow-up actions to secure agencies required mitigation plan responses; and to ensure that findings as well as actions taken are accurately documented through procedural updates.

Attached is a detailed response outlining our corrective actions.

We will continue to ensure that the requirements of Internal Revenue Code Section 6103(p)(4) and Publication 1075, *Tax Information Security Guidelines For Federal, State and Local Agencies*, are followed. If you have any questions, please contact me at 202-317-4202, or a member of your staff may contact Kevin Woolfolk, Associate Director, Safeguards at 513-975-6706.

Attachment

Attachment
TIGTA Audit # 202310007

Recommendation 1: The Chief Privacy Officer should subsequently remind agencies with late filed SSRs or CAPs of best practices at least 60 days prior to their next scheduled filing due date, and that they may request a filing extension at least 30 days before their scheduled due date if extenuating circumstances exist.

Corrective Action: The IRS agrees with this recommendation. The Safeguards office will email a reminder to the points of contact for agencies with late filed SSRs or CAPs at least 60 days prior to their next scheduled filing due date. The Office of Safeguards will issue guidance to document this ongoing requirement.

Implementation Date: November 15, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Governmental Liaison, Disclosure & Safeguards, Director (Safeguards)

Recommendation 2: The Chief Privacy Officer should offer standardized training to any new HOA on the safeguard review process and best practices for submitting agency documentation.

Corrective Action: The IRS agrees with this recommendation. The Safeguards office will email a Security and Privacy Alert to agencies publicizing the availability of standardized training for new HOAs on the safeguard review process and best practices for submitting agency documentation to be delivered using virtual meeting capabilities to deliver a presentation and to allow for a live question and answer exchange.

Implementation Date: November 15, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Governmental Liaison, Disclosure & Safeguards, Director (Safeguards)

Recommendation 3: The Chief Privacy Officer should update policies to require follow-up with State agencies concerning any unsubmitted mitigation plans after their mitigation plan due dates have passed.

Corrective Action: The IRS agrees with this recommendation. The Safeguards office will issue guidance to document the requirement to follow-up with State agencies to secure mitigation plans not submitted by established due date for submission.

Implementation Date: July 15, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Governmental Liaison, Disclosure & Safeguards, Director (Safeguards)

Recommendation 4: The Chief Privacy Officer should develop procedures to ensure that finding information is accurately documented in the PFR, SRR, and eCase as well as that case updates, case notes, relevant correspondence, and mitigation plan receipt dates are accurately documented in eCase.

Corrective Action: The IRS agrees with this recommendation. The Safeguards office will issue guidance on the procedures to follow to validate the accuracy of findings documented in the PFR, SRR, and eCase and to validate the accuracy of eCase updates, case notes, relevant correspondence, and mitigation plan receipt dates.

Implementation Date: July 15, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Governmental Liaison, Disclosure & Safeguards, Director (Safeguards)

Recommendation 5: The Chief Privacy Officer should send an annual reminder to all State agencies to notify staff of their responsibility to report data incidents within 24 hours of identification.

Corrective Action: The IRS agrees with this recommendation. The Safeguards office will email a reminder to the points of contact for agencies to notify staff of their responsibility to report data incidents within 24 hours of identification. The Safeguards office will issue guidance to document this ongoing requirement.

Implementation Date: July 15, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Governmental Liaison, Disclosure & Safeguards, Director (Safeguards)

Appendix III

Abbreviations

CAP	Corrective Action Plan
CY	Calendar Year
FTI	Federal Tax Information
HOA	Head of Agency
I.R.C.	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
PFR	Preliminary Findings Report
SRR	Safeguard Review Report
SSR	Safeguard Security Report

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.