

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Incident and Service Ticket Management Needs Improvement

May 6, 2026

Report Number: 2026-200-020

HIGHLIGHTS: Incident and Service Ticket Management Needs Improvement

Final Audit Report issued on May 6, 2026

Report Number 2026-200-020

Why TIGTA Did This Audit

An incident is an unplanned interruption to, or a reduction in the quality of, an information technology service.

The IRS categorizes incident tickets into four priority levels: Priority 1 through Priority 4. Priority 1 incidents lead to severe critical work stoppages. These incidents impact multiple internal or external customers and service to taxpayers. Priority 4 incidents are not critical. These incidents do not cause a work stoppage and there is a workaround.

We assessed whether the IRS is effectively and efficiently managing its incident management process.

Impact on Tax Administration

In Fiscal Year 2024, the IRS collected nearly \$5.1 trillion in gross taxes and processed almost 267 million tax returns and other forms, which represents a substantial amount of taxpayer personal and financial information.

When an incident occurs, it is important to resolve it effectively and within established performance goals to minimize the level of disruption to the IRS and the IRS's ability to consistently process taxpayer returns and further tax administration.

What TIGTA Found

We found that many incident tickets were unnecessary and not timely resolved. As a result, IRS employees spent time reviewing and closing the unnecessary incident tickets instead of reviewing and resolving legitimate incidents.

A significant number of incident tickets were unnecessarily generated because procedures were not followed. Specifically, nearly 20,000 of 22,600 (88 percent) of the highest priority incidents tickets (IRS refers to these as Priority 1 and 2) generated from April 2023 through September 2024 were automatically generated by a process that should have been disabled.

In addition, incident ticket resolution times exceed the IRS's target time frames. Our review of approximately 2,640 Priority 1 and Priority 2 tickets found that nearly 1,240 (47 percent) of the tickets were not resolved timely. One of the Priority 1 incidents we identified affected the Modernized Electronic Filing system. This delay impacted the system's ability to generate timely confirmations to taxpayers that the IRS received the tax return for processing at the beginning of the 2024 Filing Season for more than two weeks.

Further, approximately 4,600 tickets (of all priority levels) created between May 2023 and August 2025 were still unresolved as of August 2025. The age range of the unresolved tickets was between 4 and 572 days old, which is beyond required time frames.

Finally, the IRS did not appropriately close or migrate incident tickets from the previous incident management system. We reviewed 6,632 incident tickets that were closed in the previous system and identified 1,251 (19 percent) that were closed without any resolution. We were unable to determine if they were recreated in the new system.

What TIGTA Recommended

We made four recommendations to the Chief Information Officer, including to ensure that requests are submitted timely to turn off monitoring as required; develop enterprise-wide performance metrics to track incident resolution timeliness; ensure that data quality reviews are performed in accordance with established procedures; and reevaluate the corrective action regarding incident ticket handling requirements.

The IRS agreed with all four of our recommendations.



**TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION**

**U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024**

May 6, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Incident and Service Ticket Management Needs
Improvement (Audit No.: 2025200003)

This report presents the results of our review to determine whether the Internal Revenue Service is effectively and efficiently managing its incident management process. This review was part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Modernizing Information Technology*.

Management's complete response to the draft report is included as Appendix II. If you have any questions, please contact me or Linna K. Hung, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 2
<u>Timeliness and Accuracy of Incident Management and Ticket Resolution Remain a Concern</u>	Page 2
<u>Recommendation 1:</u>	Page 3
<u>Recommendation 2:</u>	Page 5
<u>Recommendation 3:</u>	Page 6
<u>Recommendation 4:</u>	Page 7
<u>Open Tickets Were Closed Without Resolution Prior To Migration</u>	Page 7
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 8
<u>Appendix II – Management’s Response to the Draft Report</u>	Page 10
<u>Appendix III – Glossary of Terms</u>	Page 13

Background

The Internal Revenue Service's (IRS) mission is to provide taxpayers with top quality service by helping them understand and meet their tax responsibilities and enforcing the law with integrity and fairness to all. According to the IRS Data Book, in Fiscal Year 2024, the IRS collected nearly \$5.1 trillion in gross taxes and processed almost 267 million tax returns and other forms. These tax returns and forms represent a substantial amount of taxpayer personal and financial information.¹ As the custodian of taxpayer information it is important to resolve incident tickets within established performance goals to minimize the level of disruption to the IRS and the IRS's ability to consistently process taxpayer returns and further tax administration.

According to IRS policy, an incident is an unplanned interruption to or reduction in the quality of an information technology service. Within the IRS, the User and Network Services function is responsible for overseeing the incident management program by providing service and support to information technology customers. Tickets to resolve incidents can be manually created from sources such as emails, chats, phone calls and self-service portal. In addition, tickets can be auto-generated by the IRS's enterprise monitoring system.

According to industry best practices, incident management aims to restore services as quickly as possible, and involves ensuring that incidents are properly logged, coded, and routed.² In addition, the goal of incident management should be to ensure that incidents are properly prioritized, service level agreement targets are met, and root causes are determined and addressed. Organizations like the IRS must have processes and procedures in place that reflect:

- Performance measurement.
- Request management.
- Quality improvement.
- Effective knowledge capture and distribution.
- Service level management.
- Customer experience.

These processes and procedures must be defined, documented, measurable, communicated, accessible, and understood by those who manage and execute them.

The IRS transitioned to a new incident management system

In April 2023, the IRS transitioned to a new incident management system to modernize the Information Technology workflow platform and improve the user's experience. According to the IRS, the legacy system was outdated, lacked resilience, and was not easy to manage. The new system is cloud-based and provides a centralized location for information technology support services and the capability for incidents to be updated in real time on easy-to-read dashboards. This allows employees to identify and respond to emerging issues more quickly.

¹ IRS, *Data Book, 2024*, Publication 55-B, (May 2025).

² See Appendix III for a glossary of terms.

The IRS categorizes incident tickets into four priority levels: Priority 1 through Priority 4 (hereafter referred to as P1 - P4).

- P1 incidents lead to severe critical work stoppages. These incidents impact multiple internal or external customers and service to taxpayers.
- P2 incidents refer to a major business disruption. These incidents leave critical users or groups unable to operate or cause a significant reduction in system performance.
- P3 incidents are issues that cause work stoppages for one customer with no work around.
- P4 incidents are not critical. These incidents do not cause a work stoppage and there is a workaround.

We reviewed open tickets in all four priority levels and closed tickets for P1 and P2 incidents for closed tickets due to their critical impact on IRS operations if the incidents are not timely resolved.

Results of Review

We found that many incident tickets were unnecessary and not timely resolved. As a result, IRS employees spent time reviewing and closing unnecessary incident tickets instead of reviewing and resolving legitimate incidents. In addition, we also found that some incident tickets were inappropriately closed before they migrated to a new management system. Lastly, we were unable to determine if the IRS recreated some incident tickets that were inappropriately closed in the new system.

Timeliness and Accuracy of Incident Management and Ticket Resolution Remain a Concern

A significant number of incident tickets were unnecessary because procedures were not followed

Our review of the 22,610 P1 and P2 tickets generated from April 2023 through September 2024 found that 19,968 of 22,610 (88 percent) were unnecessary because they were generated during a planned system downtime. The remaining 2,642 incident tickets were closed and will be discussed in later sections within this report. The unnecessary incident tickets were systemically generated after the IRS's automated monitoring queried another computer on the network and determined there was no connection to it. Upon further review, these tickets were associated with a planned system downtime.

The IRS's policy requires Information Technology personnel to submit a request 48 hours in advance to turn off this automated monitoring when there is a planned system downtime. However, personnel from the Enterprise Operations function confirmed that server or application owners did not follow this process. As a result, unnecessary incident tickets were generated, and IRS employees spent time reviewing and closing them instead of reviewing and resolving legitimate incidents.

Failure to follow the process of turning off automated monitoring could lead to inaccurate reporting and inefficient resource allocation. In addition, many needless incident tickets can undermine employees' confidence and delay responses to genuine incidents over time.

In response to this finding, personnel from the Enterprise Operations function stated they plan to enhance the process so automated monitoring is automatically turned off when a system downtime request is submitted.

Recommendation 1: The Chief Information Officer should ensure that requests are submitted timely to turn off monitoring as required.

Management's Response: The IRS agreed with this recommendation and stated that it has established a process, and knowledge articles are in place, to guide the use of monitoring suspension during maintenance activities. An enhancement to make the configuration item downtime field mandatory is scheduled for mid-2026.

Nearly half of the closed incident tickets reviewed exceeded target time frames

Service level management is a process that is used to measure incident and service request timeliness. Within the IRS, the Master Service Level Agreement defines incident priority levels and target resolution time frames. Incident resolution time frames vary depending on the priority level of the incident. P1 and P2 tickets require resolution within hours and P3 and P4 tickets require resolution within two to four days, respectively. Figure 1 identifies the incident priority levels and target resolution times.

Figure 1: Incident Priority Level and Target Resolution Times

Priority	Target Resolution Time
1	Within four hours
2	Within eight hours
3	Within two business days
4	Within four business days

Source: Master Service Level Agreement.³

However, our review of 2,642 closed P1 and P2 tickets created from April 2023 through September 2024 found that 1,239 (47 percent) of the tickets were not timely resolved. Failure to resolve incident tickets within the target resolution time frames may negatively impact key IRS systems and taxpayers.

³ IRS, *Internal Revenue Service Master Service Level Agreement* (January 2024).

Figure 2 shows the number of incident tickets that were not resolved within the target resolution time for the period reviewed.

Figure 2: Closed P1 and P2 Tickets Not Resolved by Target Resolution Times

Tickets	Total Number of Tickets	Number of Tickets Delayed	Age of Tickets	Average Closure Times
P1	118	101	4 – 2,756 hours	135 hours
			86 percent of tickets resolved untimely	
<p>Example of Notable Impact: The Modernized Electronic File application is a critical component of the tax filing system that provides electronic filing service for taxpayers. The untimely resolution of an incident affecting this application resulted in a backlog of returns that were not timely processed. This delay impacted the system’s ability to generate timely confirmations to taxpayers that the IRS received the tax return for processing at the beginning of the 2024 Filing Season for more than two weeks.</p>				
P2	2,524	1,138	8 – 5,399 hours	148 hours
45 percent of tickets resolved untimely				

Example of Notable Impact: One incident we reviewed affected 16,100 users of an application that allows for the exchange of tax data of multi-national enterprises between the United States and some countries and an international organization. This resulted in multiple files not successfully transmitted.

Source: Analysis of incident tickets from April 2023 through September 2024.

Thousands of incident tickets remained unresolved at the time we conducted our review

We identified 4,577 tickets created from May 2023 through August 2025 that were still unresolved as of August 2025. Further review of these unresolved tickets found that they were open between 4 and 572 days at the time of our review, which is beyond required time frames.

Figure 3 shows the breakdown and impact of the unresolved tickets.

Figure 3: Status of Unresolved Tickets

Tickets	Number Of Tickets Unresolved ⁴	Age of Tickets ⁵
P2 (Target Resolution Time within eight hours)	8	96 – 1,752 hours
Example of notable impact: 3,500 users in the Field Examination function were unable to close cases and send them to Centralized Case Processing, which is responsible for closing examined and non-examined returns and updating the Examination inventory.		
P3 (Target Resolution Time within two business days)	2,563	4 – 572 days
Example of notable impact: 1,000 users were impacted by the Electronic Fraud Detection System’s inability to move taxpayer returns out of processed status. This system is an automated system designed to detect taxpayer fraud.		
P4 (Target Resolution Time within four business days)	2,006	5 – 569 days
Example of notable impact: 10 users’ access to the Secure Access Digital Identity system at the Memphis site were impacted by one ticket. This system collects, validates, and verifies identity evidence to register applicants for IRS Online Services.		

Source: Analysis of incident tickets created from May 2023 through August 2025.

There are no established metrics to measure enterprise-wide incident management performance. If these metrics were available, management could use them to make informed decisions, drive continual improvement, and take appropriate actions to minimize disruptions. Instead, different IRS teams present different metrics to IRS leadership. While all the incident ticket information was collected, it was not all presented uniformly to IRS Associate Chief Information Officers. For example, the User and Network Services team provided monthly metrics reports focused on operational customer experience resolution times and the Enterprise Operations team reported quarterly metrics covering resolution and restoration times for application availability such as IT services and mainframe and server-related tickets.

Recommendation 2: The Chief Information Officer should develop enterprise-wide performance metrics to track incident resolution timeliness.

Management’s Response: The IRS management agreed with this recommendation and will deploy a standardized, enterprise-wide incident performance dashboard to document Information Technology handling and timeliness of priority incidents and monthly Service Level Agreement reporting.

Mandatory data that will help resolve incidents is not being captured

Our review of the 2,642 closed P1 and P2 incident tickets created from April 2023 through September 2024 identified 2,133 (81 percent) tickets that did not have an entry in the

⁴ 55 additional tickets did not contain information on the priority level.

⁵ P1 and P2 tickets are calculated in hours and P3 and P4 tickets are calculated in business days excluding weekends or holidays.

configuration item field. This field is a required entry that identifies the unique network name or asset number of the system impacted by the incident. Without capturing information for the configuration item field, the IRS may lose the ability to track repeated issues, and improve incident resolution, customer service, and efficiency.

We found that the configuration item information was missing because data quality reviews of all P1 and P2 incidents were not being completed as required. According to the IRS's procedures, a quality review should be performed before the incident ticket is closed. The IRS can either complete these data quality reviews themselves or can have a contractor conduct the reviews. We found that the contractors were voluntarily performing the data quality reviews, even though there is no contractual obligation for them to do so. The IRS also explained that staffing reductions affected the implementation of this process as part of its new system.

Recommendation 3: The Chief Information Officer should ensure that data quality reviews are performed for P1 and P2 tickets in accordance with the established procedures.

Management's Response: The IRS agreed with this recommendation and will update IRS policy to require service providers to complete mandatory P1/P2 ticket data quality controls to achieve 95 percent or greater required field completion and 100 percent review compliance.

Actions taken to address our prior recommendations were ineffective

In September 2022, we reported that incident ticket reassignments were not always justified or appropriately reassigned.⁶ The purpose of reassignments is to route the ticket to the service provider that can resolve the incident. In addition, we reported that the user's concurrence was not properly obtained before closing the tickets. A user's concurrence ensures that the incident was resolved to the customer's satisfaction before closing the incident. We recommended that the IRS ensure that incident ticket handling requirements are followed including selecting specific codes related to the issues, documenting actions taken including the reason for reassignments, and obtaining user concurrence before closing the incident ticket. The IRS agreed with our recommendation and implemented training on coding and documentation requirements.

However, we found that the IRS's corrective actions did not resolve the previously identified issues. As previously mentioned, in April 2023, the IRS transitioned to a new incident management system. Our analysis of 2,642 P1 and P2 tickets created using the new system identified the same types of concerns as reported previously. For example, we found:

- 2,556 (97 percent) tickets were closed without obtaining user concurrence.
- 805 (30 percent) tickets were reassigned between 1 and 11 times without the reason for reassignment documented.
- 502 (19 percent) tickets were closed without capturing the root cause of the issue.

When we asked personnel from the Enterprise Operations function why these conditions continued to occur, they stated that service providers are not following established guidance. They added that service providers have guidance on documenting reasons for reassignments;

⁶ TIGTA, Report No. 2022-20-053, *The End-User Incident Management Process Can Be Improved*, pp. 6-7 (September 2022).

however, not all personnel adhere to this guidance. Further, the new incident management system is not configured to validate the information entered in the reassignment field.

Recommendation 4: The Chief Information Officer should reevaluate the corrective action regarding incident ticket handling requirements and take additional steps to ensure that service providers are following incident ticket handling requirements.

Management's Response: The IRS agreed with this recommendation and will update IRS policy to standardize ticket handling requirements by service providers and ensure consistent documentation, user concurrence (where applicable), and root cause capture for P1 and P2 incidents.

Open Tickets Were Closed Without Resolution Prior To Migration

We found that the IRS did not appropriately close or migrate incident tickets from the previous incident management system. We reviewed 6,632 incident tickets that were closed in the previous system and identified 1,251 (19 percent) of the tickets were closed without any resolution. We were unable to determine if they were recreated in the new system.

IRS policy requires that incidents are properly logged and coded, reassignments are properly documented, the incident record is closed after incident resolution is successful, and customer concurrence is obtained. According to personnel from the Enterprise Operations function, they were instructed to close unresolved tickets before the legacy system was decommissioned, rather than importing or recreating incident tickets in the new system. Further, they stated that the group assigned to an issue was expected to generate new incident tickets in the new incident management system if the issue persisted. However, the IRS did not have a way to match tickets from the old system to the new incident management system.

Since there is no way for management to go back and correct these tickets, we are not making a recommendation. However, this finding highlights the necessity that the IRS follow established agency procedures during future migrations. Closing tickets without resolution may result in unaddressed incidents and impact productivity. In addition, the customer may not be notified that their ticket was closed so they could submit another ticket in the new incident management system.

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the IRS is effectively and efficiently managing its incident management process. To accomplish our objectives, we:

- Evaluated the incident management processes and practices used to resolve issues in the legacy system by reviewing incidents with the resolution status of mass closed, automatically closed, resolved with no action taken and unable to resolve.
- Determined whether the IRS is capturing, reporting, and reviewing its incident management performance metrics and timely resolving incident tickets in accordance with established timelines by reviewing the Master Service Level Agreement and IRS incident resolution timelines.
- Assessed whether the IRS's transition from the legacy system to the new incident management system met established industry standards, best practices, and guidelines by reviewing Treasury and IRS policies, procedures, guidelines, industry standards and best practices for decommissioning a system. In addition, we reviewed artifacts developed for decommissioning the legacy system to determine if they were approved timely.
- Evaluated whether the prior audit recommendation and corrective actions have been implemented by identifying and reviewing Treasury and IRS policies, procedures, guidelines and industry standards and best practices related to the identification, tracking, and closing of planned corrective actions.

Performance of This Review

This review was performed with information obtained from the Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland and Memphis, Tennessee during the period October 2024 through September 2025. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

During this review, we relied on data extracted from the legacy system and the new solution. In addition, we relied on data obtained from the IRS's User and Network Services and Enterprise Operations Divisions. To assess the reliability of the system generated data, we evaluated the data by 1) reviewing documentation about the data and the systems that produced them; and 2) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

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: processes, policies, procedures and guidelines related to the incident management process. We evaluated these controls by interviewing the Information Technology organization and business unit personnel and by reviewing incident management reports generated from both the legacy system and the new incident management system.

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

April 1, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya Kaschit D. Pandya
Chief Information Officer Pandya

Digitally signed by Kaschit D. Pandya
Date: 2026.04.01 12:22:57 -04'00'

SUBJECT: Draft Audit Report – Incident and Service Ticket Management Needs Improvement (Audit #2025200003)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. The IRS has taken and will continue to take steps to strengthen its incident management process and remains committed to continuous improvement consistent with established policies and guidelines.

Management agrees with the recommendations and will take appropriate actions to address the identified issues and improve incident management processes. Please refer to the attachment for specific details.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact me at (202) 315-5000, or a member of your staff may contact Tanya Chiaravalle, Coordinating Director, End User Digital Services, at (240) 613-4255.

Attachment

Attachment

Audit #2025200003, *Incident and Service Ticket Management Needs Improvement*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure that requests are submitted timely to turn off monitoring as required.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer has established a process, and knowledge articles are in place to guide the use of monitoring suspension during maintenance activities. An enhancement to make the CI downtime field mandatory is scheduled for mid-2026.

IMPLEMENTATION DATE: July 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 2: The Chief Information Officer should develop enterprise-wide performance metrics to track incident resolution timelines.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will deploy a standardized, enterprise-wide incident performance dashboard to document IT handling and timeliness of priority incidents and monthly SLA reporting.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

RECOMMENDATION 3: The Chief Information Officer should ensure that data quality reviews are performed for P1 and P2 tickets in accordance with the established procedures.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will update IRS policy to require service providers to complete mandatory P1/P2 ticket data quality controls to achieve ≥95% required field completion and 100% review compliance.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

Attachment

Audit #2025200003, *Incident and Service Ticket Management Needs Improvement*

RECOMMENDATION 4: The Chief Information Officer should reevaluate the corrective action regarding incident ticket handling requirements and take additional steps to ensure that service providers are following incident ticket handling requirements.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will update IRS policy to standardize ticket handling requirements by service providers and ensure consistent documentation, user concurrence (where applicable), and root cause capture for priority 1 and priority 2 incidents.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

Glossary of Terms

Term	Definition
Cloud-Based	A computing model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources, <i>e.g.</i> , network, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction.
Decommission	The removal of information technology assets from the production environment.
Incident Management	The process responsible for managing the life cycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible, and the business impact is minimized.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations. In the context of computing, it refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternative.
Metric	Something that is measured and reported to help manage a process, information technology service, or activity.
Monitoring	Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.
Priority 1	These incidents lead to severe critical work stoppage and impact on multiple internal or external customers and service to taxpayers.
Priority 2	These incidents refer to a major business disruption, critical users or groups unable to operate or a business unit experiencing significant reduction in system performance.
Priority 3	These refer to issues that cause work stoppage for one customer with no work around.
Priority 4	These are issues that are not critical where there is no work stoppage and there is a workaround.
Service Level Agreement	A document that describes the minimum performance criteria a provider promises to meet while delivering a service, typically also setting out the remedial action and any penalties that will take effect if performance falls below the promised standard.

Service Provider

Any organization that delivers a standard service or product to a customer or user. Responsible for the provisioning of products or services requested within the Service Level Agreement. Responsible for the delivery of the product or service requested by service requestor. This role is carried out by various organizations in IT and outside of IT based on products or services requested. Managers of Service Support Providers are the first level for escalation of service requests needing management oversight.



**To report fraud, waste, or abuse,
contact our hotline on the web at
<https://www.tigta.gov/reportcrime-misconduct>.**

**To make suggestions to improve IRS policies, processes, or systems
affecting taxpayers, contact us at
TIGTACommunications@tigta.treas.gov.**

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