DEPARTMENT OF THE TREASURY

WASHINGTON, D.C.

July 14, 2026

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Management Alert: Zero Paper Initiative Information Security (Audit No.: 2026208008)

This memorandum alerts you of concerns we identified at 2 sites (hereafter referred to as Site 1 and Site 2) contractors are using to support the Internal Revenue Service's (IRS) Zero Paper Initiative (ZPI). The ZPI is designed to scan and digitize paper tax forms, correspondence, and information returns. Specifically, we identified deficiencies in physical security controls designed to safeguard taxpayer data, security vulnerabilities in the information systems used to process taxpayer information, and weaknesses in information system configuration controls.

Physical Security Gaps Allowed Unauthorized Access to Restricted Areas

During our site visits, we observed that:

- 14 employees accessed areas with taxpayer information without being authorized by the IRS. These employees accessed areas where taxpayer documents were scanned, digitized, or stored on 1,375 occasions. The period of access was May through August 2025 for Site 1 and October through December 2025 for Site 2. We discussed our concerns with management officials from the Taxpayer Services function. They stated that contractors are required to review physical access logs annually. However, based on our findings, Taxpayer Services officials indicated that they may require contractors to implement a monthly review process. These reviews could help identify unauthorized employees entering restricted areas.
- The perimeter fence and the loading dock used to receive taxpayer information were open and not properly secured at Site 1. The loading dock allows entry into the facility's document storage area that contains taxpayer information. In addition, there were no guards controlling access to the area. An uncontrolled access point may allow unauthorized people to bypass other physical controls and access sensitive taxpayer information. During our discussions with contractor representatives, they stated that the loading dock is left open during the day and locked at night. Further, their contract did

not require the use of guards within the facility. We disagree. Contractors are responsible for safeguarding taxpayer data. The ZPI requires contractors to implement security controls in accordance with IRS policies.[1] These security controls are tailored for contractor information systems and sites that process taxpayer information. For example, contractors are required to limit access to areas with taxpayer information to employees with approved background investigations. In addition, Publication 4812, *Contractor Security and Privacy Controls,* includes physical security requirements for areas that contain taxpayer information. The physical security requirements include reinforced perimeters, locked buildings, and electronic security systems. Further, when a fence and gate are used to secure the perimeter, the gate should be guarded or locked with an alarm.

Management Action: The IRS plans to update the 2027 Publication 4812 to require contractors to review access logs monthly or more frequently at the discretion of the IRS.

Information System Security Vulnerabilities Were Not Timely Fixed

IRS policy requires that security vulnerabilities are prioritized and fixed based on severity. In addition, this policy defines the required time frames vulnerabilities must be fixed. Critical vulnerabilities require shorter times to fix and low security vulnerabilities have a longer time to fix. We identified critical, high, medium, and low security vulnerabilities at both contractor sites:

- Site 1 did not address security vulnerabilities within the required time frames. We identified 128 (48 percent) of 269 security vulnerabilities in information systems that process taxpayer information were not timely resolved. The IRS Cybersecurity function's limited review during the contractor security assessments would not have identified overdue vulnerabilities. Overdue vulnerabilities increase the risk that a cyberattack could compromise information systems and taxpayer information. Figure 1 shows the number of overdue vulnerabilities and the average age.

[1] IRS, Publication 4812, *Contractor Security and Privacy Controls, Handling and Protecting Information Systems Version 15*, (December 2024).

Figure 1: Security Vulnerabilities That Were Not Timely Fixed

Severity Level	Total Security Vulnerabilities	Average Age	Allowed Remediation Time
Critical	20	223 days	30 days
Example of a Critical Vulnerability: A system was using a version of software that was no longer supported by the vendor. Unsupported software will no longer receive security updates and increases the risk that the software could be exploited using known weaknesses.			
High	84	231 days	60 days
Example of a High Vulnerability: An available security update for database software was not installed. This update would fix a weakness that allows an attacker to skip the sign in steps and take actions without permission.			
Medium	19	423 days	120 days
Example of a Medium Vulnerability: An available security update was not applied. A bad actor can take advantage of this weakness to send malicious code to the system and cause services not to work.			
Low	5	504 days	180 days
Example of a Low Vulnerability: A bad actor could exploit this weakness and bypass access controls because weak communication methods are allowed.			

Source: Analysis of vulnerability scan reports provided by the IRS and IRS Publication 4812 Contractor Security and Privacy Controls.

- Site 2 used unauthorized software to scan its information systems for vulnerabilities. We found that the contractor was using open-source software that was not validated to use Security Content Automation Protocol standards.[2] IRS policy requires the use of scanning software that implements the Security Content Automation Protocol standards. In addition, this contractor did not keep records of past security vulnerabilities. Thus, the contractor did not know how long a vulnerability existed on the system. Personnel from the Cybersecurity function's Contractor Security Assessment team were aware that the Site 2 contractor was using unauthorized vulnerability scanning software. However, no actions were initiated to ensure that the contractor complied with agency requirements.

Management Action: IRS management developed a monthly process to identify unremediated aged vulnerabilities to be reviewed by procurement officials, the project office, and contractors for applicable updates.

[2] This refers to publicly accessible software that allows anyone to inspect or modify the code.

Information Systems Were Not Consistently Assessed for Secure Configuration Settings

Configuration management is the process of maintaining information systems such as computer hardware and software in the desired state. This process ensures that information systems perform in a manner consistent with expectations over time. Further, configuration settings affect the security posture or functionality of an information system. IRS policies require that information systems are scanned monthly to determine whether devices are properly configured. Additionally, the policy requires the use of authorized automated tools to assess information systems. We identified configuration vulnerabilities at both contractor sites.

- Site 1 did not scan all information systems monthly as required. Only a subset of devices was scanned each month. For example, in August 2025, only 1 of 203 devices was scanned. During contractor assessments, personnel from the IRS Cybersecurity function did not ensure that the contractor was assessing all devices monthly.
- Site 2 used unauthorized software to assess the configuration of the information system. This software did not capture sufficient details on configuration settings to determine how long a configuration weakness had existed on the system. Personnel from the Cybersecurity function's Contractor Security Assessment team were aware that the Site 2 contractor was using an unauthorized tool for configuration scanning. However, no actions were initiated to ensure that the contractor complied with agency requirements.

We provided this memorandum to the IRS for review and response. In its response, the IRS indicated that they have taken or would take corrective actions to address our concerns. We plan to visit the other contractors' facilities as they start scanning paper tax returns. We will include those results, and any actions the IRS takes to address the concerns in this memo, in our subsequent audit report.

If you have any questions, please contact me or Linna K. Hung, Assistant Inspector General for Audit (Security and Information Technology Services).