TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Direct File Pilot Deployed Successfully; However, Security and Testing Improvements Are Needed

September 23, 2024

Report Number: 2024-200-050

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

HIGHLIGHTS: The Direct File Pilot Deployed Successfully; However, Security and Testing Improvements Are Needed

Final Audit Report issued on September 23, 2024 **Report Number 2024-200-050**

Why TIGTA Did This Audit

The Inflation Reduction Act of 2022 required the IRS to establish a task force to design and report to Congress on an IRS-run free, direct electronic filing tax return system. The IRS submitted a report to Congress in May 2023 that evaluated the use of a free electronic filing system referred to as "Direct File." The Deputy Secretary of the Treasury directed the IRS to launch a limited scope pilot for the 2024 Filing Season.

This audit was initiated to assess the effectiveness of the development and security of the IRS Direct File Pilot.

Impact on Tax Administration

The Direct File Pilot launched on February 1, 2024, led by the IRS Transformation and Strategy Office with support from the Office of Information Technology. The pilot was implemented to a limited scope of taxpayers with certain types of income, credits, and deductions and who reside in one of the 12 participating piloting States. Taxpayers who live in Arizona, California, Massachusetts, or New York were also eligible to transfer their tax data to a State-supported tool to file their State tax return.

If the Direct File Pilot is not properly developed, tested, and secured, the IRS risks delays to taxpayers and submission errors. In addition, taxpayer data could be vulnerable to loss or theft.

What TIGTA Found

The IRS issued the Authorization to Operate for the Direct File Pilot with eight moderate and low risks identified during security control assessments. Also, during systems development, the Direct File Pilot team did not appropriately complete two of its required artifacts, *e.g.*, Configuration Management Plan and the About Page. Once the Authorization to Operate was issued, the Direct File Pilot team completed its first required monthly Federal Risk and Authorization Management Program *Continuous Monitoring Summary Report*. However, the report was issued without the security assessment for the cloud platform upon which the Direct File Pilot resides.

The Direct File Pilot team issued Memorandums of Understanding to participating States without relevant security or technical details for managing the exchange of taxpayer data.

The Direct File Pilot team initially developed high-level requirements in their test plan and test schedule; however, the repositories used for source code and issue tracking lacked traceability and reporting capabilities. None of the tests in the issue tracker were able to be traced back to the test plan. In addition, the Direct File Pilot contained sufficient documentation on bug, also called defect, remediation for only 12 (46 percent) of the 26 testing issues reviewed.

The Direct File Pilot complied with National Institute of Standards and Technology and IRS requirements for assessing risks associated with identity proofing and authentication and has taken steps to mitigate potential unauthorized disclosure of taxpayer data.

What TIGTA Recommended

TIGTA made six recommendations. TIGTA recommended that the Chief Information Officer should ensure that guidance provides specific policies and procedures to review and analyze artifacts during the independent verification and validation process. TIGTA also recommended that the Chief Information Officer and the Chief, Direct File, should ensure that Direct File artifacts are completed and signed prior to any future deployments; update existing Memorandums of Understanding to include security and technical details for managing the exchange of taxpayer data, and ensure that the details are included in future agreements with participating States; ensure that the requirements repository contains traceability and automatic reporting capabilities; ensure that developers document their test plan that can be traced to test types, test cases, and test results; and standardize and document procedures on how to use the requirements repository.

The IRS agreed with all six recommendations. The IRS stated it added language to guidance, signed or completed artifacts noted in this report, and updated the language in the Memorandums of Understanding with participating States. The IRS also plans to work to adopt tools that allow for automated reporting, update the Direct File test plan, and update instructions for the requirements repository.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 23, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

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

SUBJECT: Final Audit Report – The Direct File Pilot Deployed Successfully; However, Security and Testing Improvements Are Needed (Audit No.: 202320024)

This report presents the results of our review to assess the effectiveness of the development and security of the Internal Revenue Service Direct File Pilot. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Managing IRA [Inflation Reduction Act of 2022] Transformation Efforts.*

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

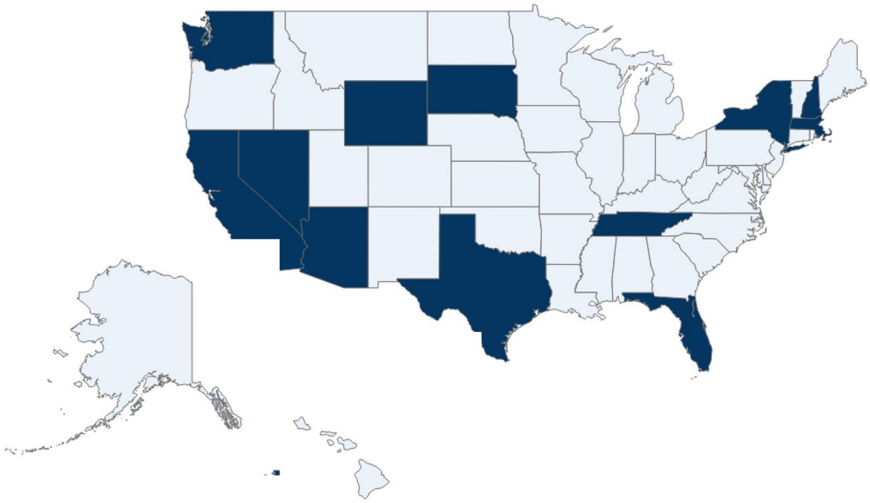
Table of Contents

Background

The Inflation Reduction Act of 2022 required the Internal Revenue Service (IRS) to establish a task force to design and report to Congress on an IRS-run free, direct electronic filing tax return system.[1] The IRS submitted a report to Congress in May 2023 that evaluated the feasibility of providing taxpayers the option to use a free IRS-run electronic filing system referred to as "Direct File." The task force is comprised of a cross-functional group of IRS employees, supported by the United States Digital Service. This task force developed a Direct File prototype to conduct user experience research and surveys. The task force used the information gathered from the prototype to compile the feasibility study report sent to Congress.

After reviewing the report, the Deputy Secretary of the Treasury issued a letter directing the IRS to launch a Direct File Pilot option for the 2024 Filing Season.[2] The pilot would gather data to further assess issues identified in the report before deciding whether to deploy a full-scale solution. The letter acknowledged that the best way to be successful is to begin with a limited scope pilot that allows the IRS to test the functionality for some taxpayers, evaluate success, and use lessons learned to inform the growth of the tool.

12 Participating States in the Direct File Pilot



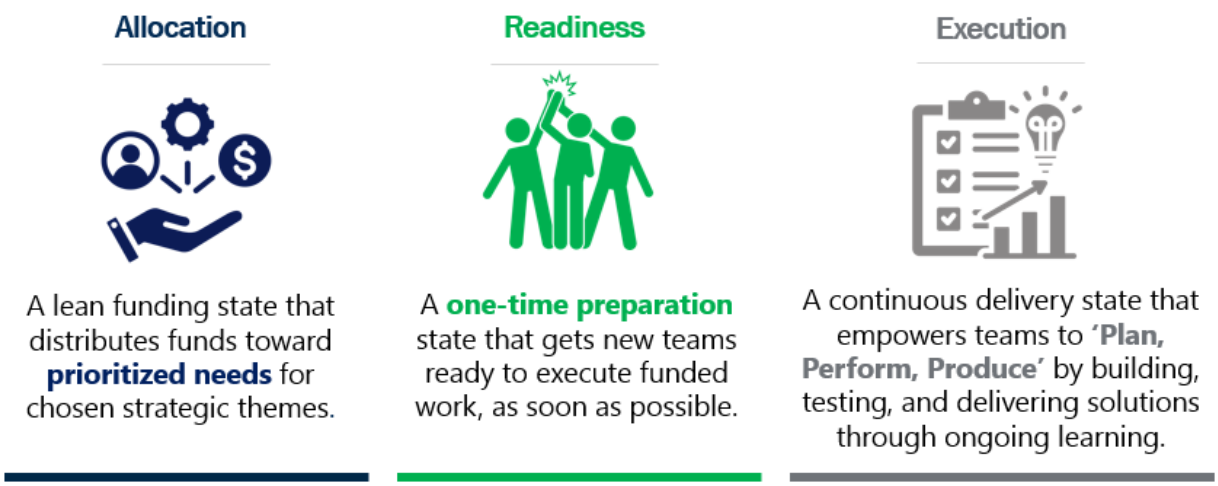
The IRS Transformation and Strategy Office, with support from the Office of Information Technology, led the team to design and deploy the Direct File Pilot. The Direct File Pilot received its Authorization to Operate (ATO) on January 23, 2024, and launched on February 1, 2024. The IRS implemented the pilot in phases throughout the 2024 Filing Season to a limited scope of taxpayers with certain types of income, credits, and deductions and who reside in the participating piloting States: Arizona, California, Florida, Massachusetts, Nevada, New Hampshire, New York, South Dakota, Tennessee, Texas, Washington, and Wyoming. Taxpayers who live in Arizona, California, Massachusetts, or New York were also eligible for the Direct File Pilot to guide them to transfer their tax data to a State-supported tool to file their State tax return.

The IRS developed the Direct File Pilot by following the One Solution Delivery Life Cycle (OneSDLC), which replaced the Enterprise Lifecycle process.[3] The OneSDLC is comprised of three states: Allocation, Readiness, and Execution, with most of the work taking place in the Execution state.

[1] Pub. L. No. 117-169, H.R. 5376-15 (B).

[2] See Appendix III for a glossary of terms.

[3] Internal Revenue Manual 2.31.1, *One Solution Delivery Life Cycle (OneSDLC) Guidance* (Jan. 23, 2023).



The OneSDLC has formal compliance and governance checkpoints during the Readiness and Execution states, in which required artifacts are to be completed. At the Readiness exit review, the product team completes compliance documentation, undergoes an independent review, and then goes before the governance board for approval to move into the Execution state. Every six months in the Execution state, the process owners review and approve compliance artifacts and the product team meets with the governance board for approval. The IRS intended to follow this process to ensure proper quality, compliance, and oversight over the development and testing of the Direct File Pilot to prevent delays to taxpayers and submission errors.

Results of Review

The Authorization to Operate Was Issued With Key Artifacts Not Appropriately Completed or Signed

The Direct File Pilot's ATO process included completing several required artifacts such as:

- System Security Plan containing the security control assessment results.
- Federal Risk and Authorization Management Program (FedRAMP) Security Threat Analysis Report (FSTAR).
- Memorandum of Understanding (MOU) with each State.
- Digital identity risk assessments.

Prior to deployment, the IRS completed its Direct File Pilot security control assessment in the FSTAR. The Direct File Pilot is located on the Integrated Enterprise Portal (IEP) infrastructure that resides on a government cloud service provider (CSP).[4] The IRS followed the National Institute of Standards and Technology (NIST) guidance, which states an initial ATO must be granted for an information system before entering the operations and maintenance phase of the system

[4] The IEP infrastructure was created to support the Information Return Intake System Web Portal and delivers web-based services for internal and external users.

development life cycle.[5] The information system's Authorizing Official will issue an ATO after an assessment of all implemented system-level controls and a review of the security status of inherited common controls as specified in security and privacy plans. The Authorizing Official will issue an ATO after reviewing the authorization package and determining whether the risk to organizational operations and assets is acceptable.

As the Direct File Pilot was in development, the IRS issued two conditional ATOs with corresponding FSTARs. The Authorizing Official issued a final ATO on January 23, 2024, and accepted a total of eight moderate and low risks identified in its FSTAR. The Direct File Pilot team created Plans of Action and Milestones for the eight risks within 60 calendar days of the signed ATO, as required by the Internal Revenue Manual (IRM).[6] The Plans of Action and Milestones for the eight risks are to be completed by June 2025.

Key system development lifecycle artifacts were not appropriately completed or signed

The Direct File Pilot exited the OneSDLC Readiness state on November 30, 2023, and entered the Execution state on December 15, 2023. A review of the Readiness state artifacts found that two (9 percent) of 22 artifacts were not appropriately completed or signed. Figure 1 describes the two incomplete artifacts.

Figure 1: Summary of Incomplete Readiness Direct File Pilot Artifacts

Artifact	Artifact Description	Artifact Issue
Configuration Management Plan	Defines and documents the scope of the information technology infrastructure to be brought under configuration control; identifies the resources, roles, and responsibilities; determines the configuration management toolsets; and provides a standard process to manage the project configuration items.	The Configuration Management Plan was not signed, as required. The Direct File Pilot team stated that the Configuration Management Plan was approved conditionally.
About Page	Contains who will be managing the project information, important points of contact, risk management, contingency management, and requirements planning.	The About Page did not contain the required contingency management plan.

Source: Treasury Inspector General for Tax Administration's analysis of OneSDLC Readiness state Direct File Pilot artifacts.

The IRS submitted two incomplete Readiness artifacts to the governance board for the exit readiness review. The Direct File Pilot's OneSDLC representative conducted an independent verification and validation review of the artifacts to ensure that they were completed and appropriately signed. The OneSDLC representative issued the Readiness memorandum stating that the project completed all artifacts and was ready for the governance board's review and approval. OneSDLC guidance states the OneSDLC representative completes an independent verification and validation review and sends the product team a signed Readiness memorandum

[5] NIST, Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Dec. 2018).

[6] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 12, 2023).

based on a validation of approved signatures.[7] The guidance does not state specific policies and procedures to follow when reviewing or analyzing the artifacts. Although the OneSDLC representative signed the Readiness memorandum, a thorough review was not performed. As a result, the governance board may have inappropriately approved the Direct File Pilot to exit the Readiness state and move into the Execution state without all Readiness artifacts completed. Without properly completing all Readiness artifacts, the IRS cannot ensure that the Direct File Pilot has undergone the required quality, compliance, and executive oversight.

Recommendation 1: The Chief Information Officer should ensure that OneSDLC guidance provides specific policies and procedures to review and analyze artifacts during the independent verification and validation process.

> **Management's Response:** The IRS agreed with this recommendation. The IRS added additional language to the coaching guide for the Life Cycle Management team that conducts Independent Verification and Validation.

Recommendation 2: The Chief Information Officer and the Chief, Direct File, should ensure that Direct File OneSDLC artifacts are completed and signed prior to future deployments.

> **Management's Response:** The IRS agreed with this recommendation. The artifacts noted in the report have been signed or completed. The IRS will follow established procedures regarding the completion and signature requirements, including exclusions or conditionals for the OneSDLC artifacts prior to opening Direct File for the 2025 Filing Season.

The MOUs were issued to participating states without detail on the security and protection of taxpayer data

When a taxpayer authorizes the Direct File Pilot to exchange information to the States, it uses a public gateway to send the appropriate data. The Direct File Pilot team selected the use of the MOUs to document the information exchanges between the IRS and each participating State. We reviewed the MOUs between the IRS and five participating states: Arizona, California, Massachusetts, New York, and Washington.

All five MOUs state that the Direct File Pilot connects the taxpayer to a State tool to fulfill their State income tax filing obligation. The pilot also provides a mechanism for the taxpayer to request and receive their own data. The MOUs state that the IRS will monitor the operation and evaluate pilot success. The State partners agreed to collaborate with the IRS on the design of a pilot, identify major risks, share user research findings, ensure launch readiness, monitor the operation of the pilot, and evaluate its success. The MOUs with Arizona, Massachusetts, and New York included additional detail that stated these participating States would work with the

[7] OneSDLC Compliance Checklist and Memo Steps (as of May 2024).

IRS to complete development and testing of a shared integration that allows the taxpayer to securely transmit their Federal return data from the Direct File Pilot to the designated State tool for purposes of filing their State income tax return, and would provide metrics and other statistical reports such as 1) a summary and detailed report on Federal tax returns by tax form type with schedules, 2) an acceptance rate, 3) rejected reasons, and 4) potential fraud indicators.

The NIST states that information exchanged via database or web-based services can use an information exchange agreement, a MOU, access or acceptable use agreement, or a non-disclosure agreement to document the exchange of information for moderate impact information systems.[8] The Direct File Pilot was categorized as moderate impact risk according to Federal Information Processing Standards.[9] For managing information exchanges, the NIST requires documenting the:

- Agreements needed to govern the exchanged information.
- Systems processing, storing, or transmitting the information.
- Roles and responsibilities of the affected organizations and users.
- Terms under which the organizations will abide by the agreement based on the team's review of relevant technical, security, administrative issues, and other appropriate requirements.

We did not find the relevant security or technical details, as defined by the NIST, required for managing the exchange of taxpayer data during our review of the MOUs with the participating States. The MOUs only contained high-level detail on how the States would work with the Direct File Pilot.

Without the appropriate agreements in place with participating States, there is a risk that the information exchange may not adequately protect sensitive data during transmission. Security failures could compromise the connected systems and the information they store, process, and transmit, thereby potentially placing Personally Identifiable Information at risk of loss or theft.

Recommendation 3: The Chief Information Officer and the Chief, Direct File, should update existing MOUs to include security and technical details for managing the exchange of taxpayer data, and ensure the security and technical details are included in future agreements with participating States.

Management's Response: The IRS agreed with this recommendation. The IRS updated the language in the MOUs with participating States to include language specific to data security and technical details for managing the exchange of taxpayer data.

Office of Audit Comment: While the stated corrective action does not ensure that future MOUs include adequate security and technical information, we reviewed the draft MOU template that will be used for future agreements with participating States and verified it contained language specific to data security and technical details for managing the exchange of taxpayer data.

[8] NIST, Special Publication 800-47, Revision 1, *Managing the Security of Information Exchanges* (July 2021).

[9] Federal Information Processing Standards, Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

Continuous Monitoring Security Reviews Were Not Fully Completed

The FedRAMP is a program that provides a standardized approach to security authorizations and continuous monitoring security assessments for the CSPs and Federal agencies. FedRAMP requires the CSP to continuously monitor its security controls, including developing and posting its continuous monitoring security artifacts to a private FedRAMP repository each month.[10] Federal agencies that leverage a FedRAMP-authorized cloud service are responsible for reviewing the CSP's artifacts to ensure that the CSP's security posture remains sufficient for their own use.

The IRS Cybersecurity function timely completed the *Direct File System Cloud Continuous Monitoring Plan* for the CSP prior to the issuance of the Direct File Pilot's ATO. The Direct File Pilot team completed and disseminated the first required monthly FedRAMP *Continuous Monitoring Summary Report* for February 2024 to the Authorizing Official for the Direct File Pilot. However, the report did not include any FedRAMP continuous monitoring security assessment information about the CSP.[11] Instead, the report states the team will be leveraging IEP contract deliverables provided by a third-party security services contractor.[12]

A successful continuous monitoring security program generates actionable data for review and to make timely risk management decisions. The IRS's *Cloud Continuous Monitoring Strategy* requires that:

- FedRAMP continuous monitoring security reviews must begin once an ATO has been issued by an Authorizing Official for an application that resides on a FedRAMP authorized CSP.
- The Information System Security Officer is responsible for reviewing the CSP's continuous monitoring security artifacts and documenting their security assessment in a monthly *Continuous Monitoring Summary Report*.
- The Information System Security Officer is also required to send the monthly *Continuous Monitoring Summary Reports* to the application's Authorizing Official who is responsible for operating an information system at an acceptable level of risk to organizational operations.
- The Authorizing Official must timely review the *Continuous Monitoring Summary Reports* to assess the level of risk of applications operating on a cloud service, make informed decisions for ongoing authorizations to operate, and ensure that the CSPs timely address or mitigate vulnerabilities identified.

[10] FedRAMP, *Continuous Monitoring Strategy Guide* (Apr. 2018), and IRS, *Cloud Continuous Monitoring Strategy* (Sept. 2022).

[11] FedRAMP continuous monitoring assessment information may include summaries of risks, vulnerabilities, Plans of Action and Milestones, and Risk-Based Decisions, along with an awareness alert from the IRS Information System Security Officer informing the Authorizing Official about potential issues with the leveraged CSP.

[12] The security services contractor is a managed services security provider for the IEP infrastructure. The security services contractor's responsibilities include conducting monthly FedRAMP continuous monitoring activities.

The Direct File Pilot team explained that they did not include the CSP continuous monitoring security information in their February 2024 report because the IEP infrastructure team is responsible for ensuring that the security services contractor continuously monitors and reports on the security of the CSP. The security services contractor develops *IEP Cloud Service Provider Continuous Monitoring Monthly Summary* reports for the IEP infrastructure team, but these monthly reports are not provided to IRS Authorizing Officials. According to the Authorizing Official for the Direct File Pilot, if potential issues are identified with the CSP, the Authorizing Official for the IEP and the contractor would verbally notify affected IRS Authorizing Official stakeholders during regularly scheduled meetings.

Verbal notification and the omission of the CSP security assessment information from the FedRAMP *Continuous Monitoring Summary Report* for the Direct File Pilot creates risk that all identified issues may not be effectively and holistically communicated to the Authorizing Official for the Direct File Pilot. This could result in IRS users not being protected against threats and vulnerabilities, thereby placing their Personally Identifiable Information vulnerable to loss or theft.

Management Action: During a meeting in March 2024, the Direct File Pilot team acknowledged the need to update their continuous monitoring process and guidance to ensure that information about the CSP contained in the monthly FedRAMP *Continuous Monitoring Summary Reports* for IRS applications that reside on the IEP infrastructure is included in the Direct File continuous monitoring report. Subsequently, the Cybersecurity function updated its continuous monitoring guidance for Information System Security Officers of applications that use the IEP infrastructure.

Security and System Testing Lacked Requirements Traceability

All information technology organizations, contractors, and other stakeholders having responsibility for developing business processes are required to conduct requirements engineering and prepare documentation. Requirements engineering involves gathering needs, validating, refining requirements, managing requirements, and prioritizing and allocating requirements.[13] The testing process involves producing system test plans, test cases, test scripts, test data, and end of test reports.[14]

Requirements planning lacked proper traceability

The Direct File Pilot team initially developed high-level requirements and testing activities in their test plan and test schedule. The Information Technology Integrated Master Schedule lists the Direct File Pilot's required tasks including testing activities and estimated completion dates. The Agile Test Strategy and Plan outlined the scope, approach, and activities necessary to effectively test and assess the quality of the Direct File Pilot. However, the plan did not include specific test scenarios, plans, or user stories. The test strategy implementation plan identified test types such as penetration testing, component testing, scenario testing, Modernized e-File acceptance testing, accessibility testing, and disaster recovery testing.

[13] IRM 2.110.2, *Requirements Engineering, Requirements Engineering Process* (Aug. 13, 2019).

[14] IRM 2.127.2, *Testing Standards and Procedures, [Information Technology] IT Testing Process and Procedures* (May 17, 2017).

The Direct File Pilot team manages testing code in the source code repository. They developed scenarios to represent a broad number of taxpayers and created test case scenarios to test the usability and accuracy of the Direct File Pilot. The scenarios in the source code repository contain links to the test cases in the issue tracker. However, the tests cases in the issue tracker cannot be traced back to the scenarios in the source code repository.

The Direct File Pilot team uses the issue tracker to create requirements, user stories, and acceptance criteria. The issue tracker uses a ticket system to track requirements, test cases, defects, and resolutions. A user can manually search through the test results, but the issue tracker does not have the capability to automate the search. According to the IRM, requirements and related artifacts should be captured and traced in a requirements repository. Without traceability, the IRS cannot ensure that all Direct File Pilot requirements were developed.

The Direct File Pilot team manually tracks requirements and testing activities using the issue tracker's issue and milestone boards. Milestone boards containing sprints and versions, corresponding to the Direct File Pilot releases, are maintained in the issue tracker. Our review of the boards found they lacked documentation on how the requirements were developed. Figure 2 shows the issues in the milestone boards were not consistently assigned a priority label, and only one of the six milestone boards allocated an open issue to a future version or sprint.

Figure 2: Issue Tracker Milestone Boards for January Through March 2024

Milestone	Date	Total Number of Issues	Number of Issues Completed	Number of Issues Prioritized	Percentage of Issues Prioritized	Number of Open Issues Allocated to Future Version or Sprint
Sprint 17	Jan. 03, 2024 – Jan. 16, 2024	210	203	161	77%	0
Sprint 18	Jan. 18, 2024 – Jan. 30, 2024	69	62	35	51%	0
Sprint 20	Feb. 14, 2024 – Feb. 27, 2024	25	22	19	76%	0
Version 23.3.0	Jan. 31, 2024 – Feb. 06, 2024	6	5	4	67%	0
Version 23.5.0	Feb. 02, 2024 – Feb. 16, 2024	97	96	94	97%	1
Version 23.9.0	Mar. 05, 2024 – Mar. 13, 2024	50	47	45	90%	0

Source: Treasury Inspector General for Tax Administration analysis of milestone boards from the Direct File Pilot's issue tracker repository as of April 19, 2024.

Testing records lacked traceability to the requirements in the test plan

The Direct File Pilot team developed and prioritized their testing requirements in the test strategy plan. However, the repositories do not automatically track or provide a report on the progress of the requirements, but instead users must manually query the repositories to find requirement information.

The Direct File Pilot team manages its testing in the issue tracker. The Direct File Pilot team defines an issue as a work item or task that an individual or team must complete and may include an 'epic' (a task with multiple work items and or teams), a new feature, a new idea to be investigated, a test scenario or a bug (also called defect) report. We reviewed a judgmental sample of 60 issues from the population of 7,254 in the issue tracker as of March 20, 2024.[15] We reviewed the sample to determine whether:

- Individual tests could be traced to the test types in the system test plan.
- Appropriate documentation exists for the tests and results, as required by the IRM.

We were unable to trace any of the issues to a test type from the test plan. When issues are created, the developers must manually assign labels to issues to provide traceability. Without properly assigning labels to issues, validation of testing requirements could not be performed to ensure that all Direct File Pilot requirements were successfully tested.

Test cases and bug remediation lack documented results

For bugs found during testing, a developer submits an issue in the repository that contains the test or steps to perform. Once a test case is created and executed, the bug is resolved, and the issue is closed. Our sample of 60 issues contained 40 closed and 20 open issues. Of the 40 closed issues, 21 were related to testing, and the remaining 19 were non-testing or duplicate issues. We found that only 10 (48 percent) of the 21 closed testing issues contained sufficient documentation to support how or why the test issue was closed.

For defects identified, the developers will submit an issue in the repository and label it as bug. The bug issues should be assigned a priority label P1, P2, or P3, with P1 being the highest priority. During our review of the issue tracker, we found that bugs were labeled priority P0 and P4. Our sample of 60 issues contained 30 bugs and 30 non-bug issues. Of the 30 bug issues, 26 were related to testing and four were duplicates or non-testing issues. Seven (27 percent) of the 26 testing issues were not assigned a priority. The remaining 19 testing issues were assigned a priority.

Also, 20 of the 26 bug issues were bugs that had been closed. Eight (40 percent) of the 20 closed bugs testing issues did not contain documentation to explain how the bug was remediated or addressed. The remaining 12 testing issues contained appropriate documentation. As a result, we determined that bug labeling and documentation were inconsistent with the bug management protocol. Failure to assign a priority to bugs can lead to them not being resolved timely and a degradation of product quality. By not accurately documenting test results, the IRS cannot ensure that all Direct File Pilot requirements were successfully tested.

The testing repository does not contain an automated reporting capability

The Direct File Pilot team uses an issue tracker to report to stakeholders on what is being tested. Testing boards for each version release contain the testing issues that can be manually queried in the issue tracker. For an upcoming version release, the source code repository shows the functions that were added and how many issues were uncovered. Although manual queries can be run in the issue tracker to look up the testing status of sprints and version releases, we did

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

not locate a documented summary report for the test types identified in the test plan. The IRM requires documented test results in a traceability repository. Test cases must be:

- Executed.
- Pass or fail.
- Documented in a traceability repository.

The test artifacts and reports must be finalized and distributed to stakeholders. Although the Direct File Pilot team is developing test cases, performing the testing, updating code, and identifying and resolving bugs, the documentation in their repositories is inconsistent, incomplete, and lacks traceability for proper reporting. As a result, the Direct File Pilot does not have proper documented testing results and is unable to ensure that the appropriate requirements are being developed and successfully tested.

The Chief Information Officer and the Chief, Direct File, should:

Recommendation 4: Ensure that the Direct File requirements repository contains traceability and automatic reporting capabilities.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will continue to manually ensure traceability of requirements per the IRM, while working to adopt tools that make reporting automated and user-friendly and accommodate the innovative style of agile software development, product management, and quality assurance that is used by Direct File.

Recommendation 5: Ensure that Direct File developers document their test plan with traceability to test types, test cases, and test results.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will update the Direct File test plan to provide additional clarification as to how Direct File development procedures support successful implementation of IRM 2.127.2.

Recommendation 6: Standardize and document procedures on how to use the Direct File requirements repository for consistency and traceability among all users.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will provide additional instructions for navigating the requirement repository in the next update to the Direct File test plan.

The Digital Identity Risk Assessment Met Federal and IRS Requirements for Authentication

The Digital Identity Risk Assessment process applies to all public-facing web applications that extend across IRS borders to resolve a specific business purpose and require authentication. The NIST provides requirements for agencies to address authentication and identity proofing risks related to digital transactions.[16] Agencies must perform risk assessments; select individual

[16] NIST, Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

assurance levels for identity proofing, authentication, and federation; determine which processes and technologies they will employ to meet each assurance level; and document these decisions.

We reviewed the Digital Identity Risk Assessment and associated documents and found that the Direct File Pilot sufficiently assessed and implemented assurance levels. The Direct File Pilot uses the Secure Access Digital Identity solution for identity proofing and authentication. The Secure Access Digital Identity solution is compliant with NIST standards at Level Two for identity proofing, authentication, and federation. All taxpayers will be required to create a Secure Access Digital Identity account to access the Direct File Pilot. By complying with NIST and IRS requirements for assessing risks associated with Direct File Pilot identity proofing and authentication, the IRS has taken steps to mitigate potential unauthorized disclosure of taxpayer data.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to assess the effectiveness of the development and security of the IRS Direct File Pilot. To accomplish our objective, we:

- Determined whether the IRS effectively addressed the system development and security requirements and other regulatory guidance by reviewing the Initial Security Assessment and Authorization package, the MOUs with participating States, and OneSDLC Readiness artifacts.
- Evaluated the effectiveness of system testing by reviewing documentation and bug remediation for a judgmental sample of 60 issues from a population of 7,254 issues in the issue tracker as of March 2024.[1] We selected our sample to ensure that our review included issues that were open and closed non-bugs and open and closed bugs. We selected a judgmental sample because we did not plan to project to the population.
- Determined whether the system met the required identity assurance level by reviewing the Direct File Pilot Digital Identity Risk Assessment documentation.
- Determined whether the operational security controls were effective by reviewing the FedRAMP continuous monitoring security reviews performed by the Cybersecurity function.

Performance of This Review

This review was performed with information obtained from the IRS Transformation and Strategy Office located in Washington, D.C., and the Cybersecurity function located at the New Carrollton Federal Building in Lanham, Maryland, during the period October 2023 through July 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 Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Kasey Koontz, Director; Myron Gulley, Audit Manager; Jamillah Hughes, Lead Auditor; David Allen, Senior Auditor; and Jonathan Elder, Manager, Data Analytics.

Data Validation Methodology

We performed tests to assess the reliability of data from the Direct File Pilot issue tracker repository. We evaluated the data by 1) reviewing existing information about the data, 2) ensuring that the information was legible and contained alphanumeric characters, 3) manually

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

tracing our sample to the source data, and 4) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for 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: Federal and IRM security and OneSDLC guidance; the requirements engineering process; and information technology testing procedures. We evaluated these controls by reviewing OneSDLC artifacts, ATO documentation, and testing documentation.

Appendix II

Management's Response to the Draft Report

COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 6, 2024

MEMORANDUM FOR DANNY R. VERNEUILLE
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel I. Werfel
Commissioner, Internal Revenue Service

Digitally signed by Daniel I. Werfel
Date: 2024.09.09 13:02:22 -04'00'

SUBJECT: Draft Audit Report – The Direct File Pilot Deployed Successfully; However, Security and Testing Improvements Are Needed (Audit No.: 202320024)

Thank you for the opportunity to review and provide comments on the subject draft audit report. We appreciate the Treasury Inspector General for Tax Administration's (TIGTA) input, analysis, and collaborative efforts to ensure the security of Direct File. In the Direct File pilot, the Internal Revenue Service (IRS) offered a completely new service to taxpayers, and in terms of technology, it was unlike anything the IRS, or other federal agencies, have offered before. In developing the pilot and now in moving forward with Direct File as a permanent option for taxpayers, security of taxpayer information is paramount. We appreciate TIGTA's recognition that the IRS has taken steps to mitigate any potential unauthorized disclosure of taxpayer data.

We thank TIGTA for their recommendations on actions we can take to further strengthen our already stringent security standards and make sure that as we move forward in expanding Direct File, we are taking all necessary steps to protect taxpayer data.

Our responses to your specific recommendations are enclosed. If you have any questions, please contact me, or a member of your staff may contact Chief, Direct File Bridget Roberts at 202-317-4212.

Attachment

Attachment

Recommendations

RECOMMENDATION 1:
The Chief Information Officer should ensure that OneSDLC guidance provides specific policies and procedures to review and analyze artifacts during the independent verification and validation process.

CORRECTIVE ACTION:
We agree with this recommendation. We have added additional language to the coaching guide for the Life Cycle Management team that conducts Independent Verification and Validation (IV&V).

IMPLEMENTATION DATE:
Implemented

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer, Strategy & Planning

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION 2:
The Chief Information Officer and Chief, Direct File, should ensure that Direct File OneSDLC artifacts are completed and signed prior to future deployments.

CORRECTIVE ACTION:
We agree with this recommendation. The artifacts noted in the report have been signed or completed. The IRS will follow established Independent Verification and Validation (IV&V) procedures regarding the completion and signature requirements, including exclusions or conditionals for One Solution Delivery Life Cycle (OneSDLC) artifacts prior to opening Direct File for the 2025 filing season.

IMPLEMENTATION DATE:
Implemented

RESPONSIBLE OFFICIAL:
Chief, Direct File

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION 3:
The Chief Information Officer and Chief, Direct File, should update existing MOUs to include security and technical details for managing the exchange of taxpayer data, and ensure the security and technical details are included in future agreements with participating States.

CORRECTIVE ACTION:
We agree with this recommendation. The IRS has updated the language in our Memorandums of Understanding (MOUs) with participating States to include language specific to data security and technical details for managing the exchange of taxpayer data.

IMPLEMENTATION DATE:
Implemented

RESPONSIBLE OFFICIAL:
Chief, Direct File

CORRECTIVE ACTION MONITORING PLAN:
N/A

The Chief Information Officer and the Chief, Direct File, should:

RECOMMENDATION 4:
Ensure the Direct File requirements repository contains traceability and automatic reporting capabilities.

CORRECTIVE ACTION:
We agree with this recommendation. The IRS will continue to manually ensure traceability of requirements per Internal Revenue Manual (IRM) 2.110.1, Requirements Engineering (RE) Directive, while we work to adopt tools that both make reporting automated and user-friendly and accommodate the innovative style of agile software development, product management, and quality assurance that is used by Direct File.

IMPLEMENTATION DATE:
February 15, 2026

RESPONSIBLE OFFICIAL:
Chief, Direct File

CORRECTIVE ACTION MONITORING PLAN:
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 5:
Ensure that Direct File developers document their test plan with traceability to test types, test cases, and test results.

CORRECTIVE ACTION:
We agree with this recommendation. The next update to the Direct File test plan will provide additional clarification as to how Direct File development procedures support successful implementation of Internal Revenue Manual (IRM) 2.127.2, IT Testing Process and Procedures.

IMPLEMENTATION DATE:
February 15, 2025

RESPONSIBLE OFFICIAL:
Chief, Direct File

CORRECTIVE ACTION MONITORING PLAN:
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 6:
Standardize and document procedures on how to use the Direct File requirements repository for consistency and traceability among all users.

CORRECTIVE ACTION:
We agree with this recommendation and will provide additional instructions for navigating the requirement repository in the next update to the Direct File test plan.

IMPLEMENTATION DATE:
February 15, 2025

RESPONSIBLE OFFICIAL:
Chief, Direct File

CORRECTIVE ACTION MONITORING PLAN:
We will monitor this corrective action as part of our internal management control system.

Appendix III

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization to Operate	The management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorizing Official	An official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Bug	A defect, imperfection, or malfunction in a computer program.
Cloud	The use of computing resources, *e.g.*, hardware and software, which are delivered as a service over a network (typically the Internet).
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Criteria	A standard of judgment or criticism; a rule or principle for evaluating or testing something.
Defect	An error in coding or logic that causes a program to malfunction or to produce incorrect/unexpected results.
Digital Identity Risk Assessment	This process identifies the risks to system security and determines the probability of occurrence, the resulting impact, and the additional safeguards that would mitigate the impact. It is a redesign of the IRS's previous Electronic Authentication Risk Assessment process.
Disaster Recovery Testing	A full scale, functional exercise that involves recovering the system or application on nonproduction equipment, in a simulated environment, or at the recovery location.
Federal Information Processing Standards Publication 199	Standards for categorizing information and information systems, which establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems.
Federal Risk and Authorization Management Program	A Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Term	Definition
Federation	A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.
Governance Board	Exists to ensure that the program goals are achieved and that the program and component projects are delivering within their defined scope, schedule, and budget. In addition, the governance board approves risk response plans and milestone exits and resolves escalated issues.
Identity Proofing	Verifying the claimed identity of an applicant by collecting and validating sufficient information, *e.g.*, identity history, credentials, and documents, about a person.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS. The Manual contains the directions employees need to fulfill their operational responsibilities.
Issue Tracker	A web-based repository that uses a ticket system to create requirements; user stories; and acceptance criteria, test cases, defects, and resolutions.
Memorandum of Understanding	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
Milestone	A management decision point placed at a natural breakpoint in the life cycle, at the end of the phase, where management determines whether a project can proceed to the next phase.
Modernized e-File	A web-based platform for filing approximately 330 forms to the IRS. It serves to streamline filing processes and reduces the costs associated with a paper-based process.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are name, Social Security Number, date of birth, place of birth, address, and biometric record.
Pilot	A limited version (limited functionality or limited number of users) of a system being deployed to discover as well as resolve problems before full implementation.
Protocol	A set of rules and formats, semantic and syntactic, permitting information systems to exchange information.
Requirement	Describes a condition or capability to which a system must conform, either derived directly from user needs or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Risk	A potential event or condition that could have an impact or opportunity on the cost, schedule, business, or technical performance of an information technology investment, program, project, or organization.

Term	Definition
Secure Access Digital Identity	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. Security Access Digital Identity is a major system that will deliver a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
Security Control	A safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. The goal of each sprint is to get a subset of the project's functionality to a "production-ready" state.
Test Case	A documented set of actions performed on a system to determine if it satisfies software requirements and functions correctly. The purpose of a test case is to determine if different features within a system are performing as expected and to confirm that the system satisfies all related standards, guidelines, and customer requirements.
Traceability	Describes the life of a requirement from the initial source through its development and actual deployment into operations.
User Stories	Short, simple descriptions of a need told from the perspective of the person who desires the new functionality, usually a user or customer of the system.
Vulnerabilities	Weaknesses in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

Appendix IV

Abbreviations

ATO	Authorization to Operate
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FSTAR	Federal Risk and Authorization Management Program Security Threat Analysis Report
IEP	Integrated Enterprise Portal
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OneSDLC	One Solution Delivery Life Cycle

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.