Audit Report

OIG-26-032

GOVERNMENT-WIDE FINANCIAL SERVICES

Fiscal Service's Sensitive Payment Systems' Controls are Generally Adequate but Weaknesses and Deficiencies Exist

June 8, 2026

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

Contents

Audit Report

Appendices

Abbreviations

BETC	Business Event Type Code
CO	Certifying Officer
CUI	Controlled Unclassified Information
DEO	Data Entry Operator
DLP	Data Loss Prevention
DO	Designating Official
Fiscal Service	Bureau of the Fiscal Service
GAO	Government Accountability Office
Green Book	*Standards for Internal Control in the Federal Government*
IDD	International Direct Deposit
IT	information technology
ITS.gov	International Treasury Services
JAMES	Joint Audit Management Enterprise System
NIST	National Institute of Standards and Technology
NTDO	Non-Treasury Disbursing Office
OFAC	Office of Foreign Assets Control
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAM	Payment Automation Manager
PII	personally identifiable information
PRF	Payment Request File
SOP	Standard Operating Procedure

SP	Special Publication
SPS	Secure Payment System
TAS	Treasury Account Symbol
TDO	Treasury Disbursing Office
TIN	Taxpayer Identification Number
TOP	Treasury Offset Program
Treasury	Department of the Treasury

This Page Intentionally Left Blank

Audit Report

June 8, 2026

Joseph Gioeli
Acting Commissioner
Bureau of the Fiscal Service

This report presents the results of our audit of the Bureau of the Fiscal Service's (Fiscal Service) sensitive payment systems. Our audit objectives were to (1) determine the adequacy of controls in place for granting or restricting access to Fiscal Service's sensitive payment systems; (2) determine the adequacy of controls in place to ensure payments are made in accordance with federal laws, regulations, and guidance; and (3) follow up on any allegations of improper or fraudulent payments made by Fiscal Service.

To accomplish our objectives, we reviewed applicable laws, regulations, directives, standard operating procedures (SOPs), and guidance; and interviewed Fiscal Service officials and personnel. We tested the process for granting and restricting user access; and whether access-related internal controls were properly designed, implemented, and operating effectively. We also tested whether payments processed through Fiscal Service's sensitive payment systems were duly certified; the removal of payments from a system was properly authorized; and internal controls for payments were properly designed, implemented, and operating effectively. The scope of our audit covered the period from October 1, 2024, through February 28, 2025, for access-related fieldwork; and December 1, 2024, through March 16, 2025, for payment-related fieldwork. Additionally, we obtained testimonial evidence from Fiscal Service officials to determine if they are aware of any allegations of improper or fraudulent payments covering October 1, 2024, through March 16, 2025, as well as fiscal years 2023 and 2024. The following Fiscal Service systems were included in our scope: the Secure Payment System (SPS), the Payment Automation Manager (PAM), and International Treasury Services (ITS.gov). We conducted fieldwork from May 2025

through March 2026. Appendix 1 contains a more detailed description of our objectives, scope, and methodology.

Results in Brief

Fiscal Service generally has adequate access and payment-related controls in place, and there were no specific allegations of improper or fraudulent payments.

While Fiscal Service generally followed relevant policies and SOPs for granting and restricting access to its sensitive payment systems, weaknesses exist. Specifically, Fiscal Service did not document the procedures for modifying users' access to the PAM database in the *PAM Access Management* SOP and did not provide a Rules of Behavior form to a Department of the Treasury (Treasury) employee before granting that employee access to Fiscal Service's infrastructure, PAM, and SPS.

In addition, Fiscal Service's Data Loss Prevention (DLP) solutions[1] did not prevent a Treasury employee with access to Fiscal Service's sensitive payment systems from transmitting personally identifiable information (PII) externally to another federal agency. We also noted that Fiscal Service inadvertently provided a Treasury employee read and write access[2] to the SPS database instead of read-only access because of human error. This error was detected and corrected the day after the mistaken access level was provided and was not used by the Treasury employee.

Related to payments, while controls in Fiscal Service's sensitive payment systems were properly designed, implemented, and operating effectively, we identified weaknesses and deficiencies that resulted in potential and confirmed improper payments, failure to adhere to federal law and regulations, and wasted federal resources. For ITS.gov, Fiscal Service did not properly withhold funds to collect delinquent debts from payments disbursed and issued duplicate payment schedules because Fiscal Service

[1] DLP solutions are security solutions that identify and help prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

[2] Read and write access allows a user to read the data saved in an information system and modify, delete, or add data to the system. Read-only access only allows a user to read the data saved in an information system.

lacked controls to prevent Non-Treasury Disbursing Office (NTDO) agencies from using duplicate payment schedule numbers.[3] For payments disbursed through PAM, Fiscal Service lacked controls to prevent agencies from submitting payee information with clearly invalid Taxpayer Identification Numbers (TIN).[4] In addition, Fiscal Service validated incomplete payment authority delegation and designation forms.

Accordingly, we are making 9 recommendations to improve Fiscal Service controls over its access and payment processes. We recommend that the Acting Commissioner of Fiscal Service (1) update the *PAM Access Management* SOP to include procedures for modifying users' access to the PAM database; (2) ensure Fiscal Service personnel adhere to Treasury policy and follow Fiscal Service onboarding procedures to ensure all users sign a Rules of Behavior form before granting them access to Fiscal Service's systems and infrastructure; (3) evaluate the existing configuration of the DLP solutions to determine whether additional security controls are necessary to mitigate the risk of unsecured external transmission of low-risk PII[5] and implement any additional identified security controls; (4) update Fiscal Service's *Email and Instant-Messaging Policy* to provide clarity on when low-risk PII constitutes Controlled Unclassified Information (CUI)[6] and disseminate the updated policy to all applicable Fiscal Service personnel; (5) implement a control to ensure all eligible Treasury Disbursing Office (TDO) payments disbursed through ITS.gov are matched against the Treasury Offset Program (TOP)[7] database; (6) implement a control for ITS.gov payments to ensure that an NTDO cannot enter duplicate payment schedule numbers into ITS.gov within the same fiscal year; (7) implement a control to reject any payments with clearly invalid TINs and make the

[3] A payment schedule is a grouping of payments that can include one or multiple payments that are the same payment type and payment method and must be disbursed simultaneously.

[4] A TIN is a nine-digit unique identification number. A TIN may be a Social Security Number or another number, such as an Employer Identification Number.

[5] Fiscal Service, Policy 301-2*, Email and Instant Messaging Policy* (August 18, 2024), p. 3, categorizes the following as low-risk PII: name, email address, phone number, and physical home address.

[6] CUI is sensitive, non-classified information created or possessed by the government, or on its behalf, that requires specific safeguarding and dissemination controls.

[7] TOP is a centralized federal program, administered by Fiscal Service, that collects delinquent debts owed to federal and state agencies by intercepting, or "offsetting," federal payments such as tax refunds, federal pay, or benefit payments.

agencies resubmit the payments with valid TINs; (8) issue guidance to agencies explaining the importance of inputting TINs accurately, and include in the guidance a requirement that agencies notify Fiscal Service of the need to use clearly invalid TINs; and (9) implement a supervisory control to ensure Fiscal Service personnel adhere to policy and validate only complete payment authority delegation and designation forms.

Fiscal Service officials did not make any allegations of improper or fraudulent payments during our audit. However, we found improper payments and identified related control deficiencies. We did not find evidence of violations of administrative or criminal law that would constitute fraud.

As a matter of concern, there are discrepancies between PAM and SPS records. It is prudent for Fiscal Service officials to minimize data discrepancies between the two systems.

In a written response, included in its entirety as appendix 2, Fiscal Service management concurred with the goals underpinning all nine recommendations and provided their planned and taken corrective actions. We have not verified Fiscal Service management's corrective actions taken, but the stated corrective actions meet the intent of our recommendations. Management should include its planned corrective actions and expected completion date(s) in the Joint Audit Management Enterprise System (JAMES).

In response to recommendations 1, 2 and 4, management stated they have implemented or plan to implement new SOPs and/or policies. For recommendation 3, management stated they plan to evaluate the configuration of the DLP solutions to determine whether additional controls are necessary. For recommendation 5, management stated they intend to implement enhancements to their international payment systems in the future. For recommendation 6, management stated they will implement a control to prevent agencies from submitting duplicate payment schedule numbers. Management also stated that any error resulting in an improper payment was due to the payor agency's failure to properly verify the accuracy and legitimacy of its payment before certifying the payment to Fiscal Service for processing. For recommendations 7 and 8, management stated they are evaluating solutions to implement TIN verification screening functionality and

will issue guidance to agencies emphasizing the need to accurately input TINs. For recommendation 9, management stated they implemented a supervisory control over approval of payment authority delegation and designation forms.

Background

Fiscal Service's mission is to promote the financial integrity and operational efficiency of the U.S. Government and is its central disbursing agency. In fiscal year 2025, Fiscal Service disbursed nearly 1.3 billion payments on behalf of more than 250 federal entities, totaling over $6 trillion, accounting for more than 88 percent of all federal payments that fiscal year.

Disbursing Authority

Under federal law, the authority to disburse public money available for expenditure by an executive agency is primarily centralized within Treasury, though certain other agencies have their own disbursing officials.[8] The Secretary of the Treasury may also delegate this authority to officers and employees of other executive agencies. Agencies that do not have disbursing authority must submit schedules to Fiscal Service for payments to be drawn on the Treasury. A TDO is a Fiscal Service office that disburses payments as instructed by authorized agency officials. An NTDO is an office at a federal entity that retains its own disbursing authority and for which Fiscal Service issues payments through Fiscal Service systems. As the Federal Government's central disbursing agency, Fiscal Service maintains multiple sensitive payment systems, such as SPS, PAM, and ITS.gov, that manage disbursements.

Secure Payment System

SPS is a system used by payor agencies to request payments to be disbursed through PAM and ITS.gov and to provide a legal authorization for Fiscal Service to make payments on its behalf, in accordance with 31 U.S.C. § 3325(a). SPS provides agencies with

[8] 31 U.S.C. § 3321, *Disbursing authority in the executive branch*

the capability to create and submit electronic payment certifications to Fiscal Service, and for Fiscal Service to validate and authenticate the certifications before disbursement. To submit payment schedules to SPS, a federal entity must involve two distinct user roles: a Data Entry Operator (DEO),[9] who creates the payment schedule and a Certifying Officer (CO),[10] who examines and approves (certifies) the payment schedule. Payment schedules certified in SPS are sent to PAM or ITS.gov for disbursement.

Payment Automation Manager System

PAM is a payment processing system that enables federal agencies to make domestic payments. The system accepts and validates payment schedules and issues automated clearing house, check, instant, and wire disbursements for agencies with domestic payments disbursed by TDOs. PAM processes more than a billion payments annually. In addition to processing payments, PAM passes payment-related data to interfacing applications that account for and store this information.

International Treasury Services Payment System

ITS.gov is a cross-border payment and collection system, developed and operated jointly by the Federal Reserve Bank of Kansas City and Fiscal Service. The ITS.gov application is a platform that enables federal agencies to make international payments to more than 248 countries in 152 currencies. ITS.gov also enables federal agencies to issue both U.S. dollar and foreign currency payments electronically using various networks; and supports international payments for both TDOs and NTDOs. Agencies using TDOs certify payments in SPS to be disbursed through ITS.gov on their behalf. NTDOs do not use SPS and instead submit payment schedules and certifications directly to ITS.gov.

[9] A DEO is an agency official or employee designated with the authority to create and edit payment schedules using SPS.

[10] A CO is the official within an agency or organization that is responsible for verifying that payments made by the Federal Government are legal, proper, and correct.

Information System Security

The Federal Information Security Modernization Act of 2014[11] requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency. Treasury policy states that all Treasury information technology (IT) systems involved in the generation, storage, processing, transfer, display, or communication of non-national security information must be protected at a level commensurate with the potential impact of a loss of confidentiality, integrity, or availability on organizations' operations, assets, or individuals.[12] Each non-national security information system is assigned a potential impact[13] level using Federal Information Processing Standards 199 and the corresponding requirements, using Federal Information Processing Standards 200 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.[14]

NIST SP 800-53 requirements include a list of access controls which, when properly implemented, ensure a level of protection that matches the criticality and sensitivity of the information and information system. Fiscal Service establishes the minimum security requirements for its information systems, including access controls, in its *Baseline Security Requirements* document, and records the controls that have been implemented, or are planned for implementation, in each sensitive payment system's *Security Controls Matrix*.

Treasury Offset Program

Fiscal Service administers TOP to collect delinquent debts owed to federal agencies and participating states by withholding federal payments owed to debtors, as required by 31 U.S.C. § 3716 and 31 CFR 285.4 and 285.5. Before issuing a payment, disbursing

[11] P.L. 113-283 (December 18, 2014)

[12] Treasury, Department Publication 85-01, Volume 1, *Treasury Information Technology Security Program* (February 28, 2022), p. 20

[13] Potential impact is the loss of confidentiality, integrity, or availability that could be expected to have an adverse effect on the organization or individuals.

[14] NIST, SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations" (Sept. 2020)

officials compare a payee's name and TIN to information about debtors in the TOP database. Fiscal Service refers to this comparison process as "matching." When a match occurs, TOP withholds funds, to the extent allowed by law, from the payee to pay the delinquent debt. Fiscal Service collects fees annually from amounts offset and paid to the state and federal agencies to cover its costs for collections through TOP.

Improper Payments

Fiscal Service plays a role in leading government-wide efforts to identify, prevent, and recover improper payments,[15] as required by Executive Order 14249.[16] The Payment Integrity Information Act of 2019[17] modernized payment integrity and improper payment requirements for executive agencies. The Office of Management and Budget (OMB) issued Circular A-123, Appendix C,[18] to implement the requirements of the Payment Integrity Information Act of 2019 and establish internal control guidance for federal agencies specific to improper payments. OMB Circular A-123, Appendix C, requires that programs implement internal controls to prevent and detect improper payments. As such, Fiscal Service officials are responsible for implementing internal controls to prevent and detect improper payments in its payment systems.

Audit Results

Access Controls

Fiscal Service controls are generally adequate and Fiscal Service personnel followed relevant policies and procedures for granting and removing access for 19 of 20 users who had access to PAM,

[15] An improper payment, as defined by 31 U.S.C. § 3351(4)(a), is any payment that should not have been made or that was made in an incorrect amount, including an overpayment or underpayment, under a statutory, contractual, administrative, or other legally applicable requirement, to include any duplicate payment.

[16] Executive Order 14249, "Protecting America's Bank Account Against Fraud, Waste, and Abuse" (March 25, 2025)

[17] 31 U.S.C. §§ 3351–3358

[18] OMB, Circular A-123, Appendix C, *Requirements for Payment Integrity Improvement* (March 5, 2021)

SPS, or ITS.gov from October 1, 2024, through February 28, 2025. However, Fiscal Service did not document the procedures for modifying users' access to the PAM database in the *PAM Access Management* SOP; and did not provide a Rules of Behavior form to a Treasury employee before granting that employee access to Fiscal Service's infrastructure, PAM, and SPS, as required by federal IT standards and Treasury policy. Additionally, Fiscal Service's DLP solutions did not prevent a Treasury employee with access to Fiscal Service's sensitive payment systems from transmitting PII externally to another federal agency.

We noted that Fiscal Service inadvertently provided a Treasury employee read and write access to the SPS database instead of read-only access because of human error. Specifically, on January 31, 2025, Fiscal Service's Enterprise IT Operations Division mistakenly granted read and write access to the Treasury employee. They detected and corrected the error on February 1, 2025. The Treasury employee first accessed SPS database during Fiscal Service's guided walkthrough of SPS on February 5, 2025, and therefore, the elevated access level was not used by the Treasury employee. As such, we do not consider this a finding.

Finding 1 Fiscal Service Did Not Document the Procedures for Modifying Users' Access to the PAM Database

Fiscal Service did not document the procedures for modifying users' access to the PAM database in the *PAM Access Management* SOP, as required by the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book). Green Book Attribute 3.09–3.11, *Documentation of the Internal Control System*, states that management should develop and maintain documentation of its internal control system to communicate all aspects of internal control execution, and to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel.[19] A Fiscal Service official told us that the procedures for modifying users' access to the PAM database are generally

[19] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, (Sept. 2014), p. 29

understood internally, but these procedures are not documented in the *PAM Access Management* SOP.

A lack of documented procedures for modifying users' access to the PAM database exposes Fiscal Service to significant risks across security, legal, and operational areas. PAM processes roughly 88 percent of all federal payments and their associated data, therefore, misuse or damage to the PAM database, such as corrupting or deleting data in the database, is a higher security and privacy risk than other Fiscal Service systems. Negligence of access controls could lead to data breaches and system outages. For instance, users receiving access that exceeds their job requirements may inadvertently or intentionally misuse or damage the PAM database, potentially compromising sensitive information and organizational integrity. Documenting all aspects of modifying access in the *PAM Access Management* SOP retains organizational knowledge and mitigates the risks of inadvertent or unauthorized access and misuse or theft of data.

Recommendation

We recommend that the Acting Commissioner of Fiscal Service:

1. Update the *PAM Access Management* SOP to include procedures for modifying users' access to the PAM database.

Management Response

Fiscal Service management concurs and stated they implemented our recommendation by migrating the PAM database off the mainframe and modernized and standardized its access control procedures through a new enterprise-level SOP that applies to all database platforms.

OIG Comment

We have not verified Fiscal Service management's corrective actions taken, but the stated corrective actions meet the intent of our recommendation. Management should record its corrective actions and completion date(s) in JAMES.

Finding 2 Fiscal Service Did Not Provide a Rules of Behavior Form Prior to Granting Access to Fiscal Service's Sensitive Payment Systems and Infrastructure

Fiscal Service did not provide a Rules of Behavior form[20] to a Treasury employee prior to granting the employee access to Fiscal Service's sensitive payment systems and infrastructure. After the employee was granted access to Fiscal Service's infrastructure, including PAM and SPS, the Deputy Assistant Commissioner, Enterprise IT Operations, provided the employee with a Rules of Behavior form for those systems. Fiscal Service officials told us this occurred because the Treasury employee did not go through Fiscal Service's normal onboarding process, which includes acceptance of the Rules of Behavior.

NIST SP 800-53 and Treasury policy require organizations to establish rules describing user responsibilities and expected behavior for information and system usage, security, and privacy, and to provide the rules to individuals requiring access to the system.[21] They also require organizations to receive documented acknowledgment from individuals requiring access to the system, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.

Without being provided with the Rules of Behavior form and signing its acceptance, users may not know their responsibilities for properly securing and using Fiscal Service data, equipment, IT systems, and facilities. Furthermore, it exposes Fiscal Service to significant risks across security, legal, and operational areas. Fiscal Service may also face regulatory penalties in the event of a security breach or misuse of data, for which Fiscal Service may not be able to take disciplinary action against a user for a policy violation.

[20] The Fiscal Service Rules of Behavior form is required for those users who access or maintain any Fiscal Service data, equipment, IT systems, or facilities.

[21] NIST, SP 800-53, Revision 5, PL-4, *Rules of Behavior*, p. 197; Treasury, Directive Publication 85-01, Vol. 1, Appendix A, *Minimum Standard Parameters for Non-National Security Information and Information Systems* (February 28, 2022), pp. E-1

Recommendation

We recommend that the Acting Commissioner of Fiscal Service:

1. Ensure Fiscal Service personnel adhere to Treasury policy and follow Fiscal Service onboarding procedures to ensure all users sign a Rules of Behavior form before granting them access to Fiscal Service's systems and infrastructure.

Management Response

Fiscal Service management concurs and will update their policies to explicitly state that the Rules of Behavior apply to all users, regardless of the employer, who access any Fiscal Service data, and will require either a signed form or system-verified completion of the Rules of Behavior training module prior to gaining access to Fiscal Service systems.

OIG Comment

Fiscal Service management's planned corrective actions meet the intent of our recommendation. Management should include its planned corrective actions and expected completion date(s) in JAMES.

Finding 3 Fiscal Service Improperly Transmitted Protected Personally Identifiable Information

Fiscal Service's DLP solutions did not prevent a Treasury employee with access to Fiscal Service's sensitive payment systems from transmitting low-risk PII externally to another federal agency. Specifically, the Treasury employee emailed a spreadsheet consisting of names and businesses associated with payment amounts outside of Treasury. While the employee attempted to secure the low-risk PII by changing the file extension of the spreadsheet and password protecting the file, the employee did not properly encrypt the spreadsheet or use the proper form to get approval from Fiscal Service's Chief Information Security Officer for sending PII externally, as required by Fiscal Service's *Email and Instant Messaging Policy*.

Fiscal Service employs various DLP solutions to monitor the distribution of PII. The DLP solutions Fiscal Service has in place can be configured to prevent the movement of low-risk PII data by using customizable data classification and risk-based enforcement policies. It can also be configured to allow Fiscal Service officials to define what constitutes low-risk PII data within its specific environment, and tailor controls accordingly. However, the current DLP solutions were not configured to prevent transmissions with low-risk PII.

In addition, the *Email and Instant-Messaging Policy* did not clearly document when low-risk PII would be classified as CUI versus standard low-risk PII. There is a critical distinction between those two categories within the policy because CUI low-risk PII requires additional protections, including encrypting the PII and receiving approvals for transmitting PII externally, whereas low-risk PII can be transmitted without additional protections and approvals. GAO's Green Book Attribute 12.02, *Documentation of Responsibilities through Policies*, states that management should document in policies the internal control responsibilities of the organization.[22] As a result of the contradictory guidance regarding the classification of low-risk PII within Fiscal Service's *Email and Instant-Messaging Policy*, users may not know what steps they need to take to transmit PII externally. Failure to clarify classification criteria for low-risk PII exposes Fiscal Service to regulatory non-compliance, financial penalties, reputational damage, and increased likelihood of identity theft or fraud.

Recommendations

We recommend that the Acting Commissioner of Fiscal Service:

1. Evaluate the existing configuration of the DLP solutions to determine whether additional security controls are necessary to mitigate the risk of unsecured external transmission of low-risk PII and implement any additional identified security controls.

[22] GAO, Green Book, p. 56

Management Response

Fiscal Service management concurs and will evaluate the existing configuration of the DLP solutions.

OIG Comment

Fiscal Service management's planned corrective actions meet the intent of our recommendation. Management should include its planned corrective actions and expected completion date(s) in JAMES.

2. Update Fiscal Service's *Email and Instant-Messaging Policy* to provide clarity on when low-risk PII constitutes CUI and disseminate the updated policy to all applicable Fiscal Service personnel.

Management Response

Fiscal Service management concurs and will update and disseminate its policies to provide clarity on low-risk PII.

OIG Comment

Fiscal Service management's planned corrective actions meet the intent of our recommendation. Management should include its planned corrective actions and expected completion date(s) in JAMES.

Payment Controls

We reviewed the significant internal controls in SPS, PAM, and ITS.gov to ensure that payments are made in accordance with federal laws, regulations, and guidance. In general, controls were designed, implemented, and operating effectively. However, we identified weaknesses and deficiencies that resulted in potential and confirmed improper payments, failure to adhere to federal law and regulations, and wasted federal resources. Specifically, for ITS.gov, Fiscal Service did not match payments it disbursed against the TOP database, and therefore did not properly withhold funds to collect delinquent debts. Also, Fiscal Service issued duplicate payments because ITS.gov lacked controls to prevent NTDO

agencies from using duplicate payment schedule numbers. For payments disbursed through PAM, Fiscal Service lacked controls to prevent agencies from submitting payee information with clearly invalid TINs, preventing Fiscal Service from performing offsets and collecting delinquent debt. Additionally, Fiscal Service did not have controls in place to ensure Fiscal Service personnel validated only complete payment authority delegation and designation forms. As a matter of concern, there are data discrepancies between PAM and SPS records.

Fiscal Service officials did not make any allegations of improper or fraudulent payments during our audit. However, we found improper payments and identified related control deficiencies. We did not find evidence of violations of administrative or criminal law that would constitute fraud.

Finding 4 Fiscal Service Did Not Collect Delinquent Debts Before Disbursing International Payments

Fiscal Service did not properly withhold funds to collect delinquent debts from payments TDOs disbursed through ITS.gov, as required by federal law and regulations. Federal law requires Treasury to withhold all or part of federal payments made to persons who owe delinquent nontax debts to satisfy the debts.[23] This process is referred to as an "offset." 31 CFR 285.4 and 285.5 require disbursing officials, like TDOs, to compare payments with delinquent debt records and to reduce payments to collect those debts. In addition, OMB Circular A-123, Appendix C, states that all programs must proactively manage their payment integrity risk to prevent improper payments.[24]

Fiscal Service did not collect the debts because it does not have an internal control in ITS.gov to match the TDO payments[25] it disburses against the TOP database. Fiscal Service officials told us ITS.gov currently lacks the capability to screen international

[23] 31 U.S.C. § 3716(c). See also 31 CFR 285.4 and 285.5
[24] OMB, Circular A-123, Appendix C, p. 28
[25] Fiscal Service is not responsible for matching NTDO payments against the TOP database.

payments for offset. Fiscal Service intends to implement enhancements to ITS.gov in the future.

In our audit scope, Fiscal Service disbursed more than one million TDO International Direct Deposit (IDD)[26] payments through ITS.gov, totaling nearly $1 billion. Thus, we asked Fiscal Service to analyze those TDO IDD payments for three agencies to determine how many of these payments would have resulted in matches against TOP.[27] Fiscal Service officials told us that based on that analysis, over 13,000 payments, totaling more than $18 million, were disbursed within our scope period to beneficiaries with debt recorded in TOP. Fiscal Service officials told us that not all payments with TOP matches are eligible for offset, and offset amounts per payment vary, so not all of the $18 million in payments would be improper. Because the dates of these payments do not align with the date of the TOP data used for comparison and the query was specific to TDO IDD payments, we also cannot extrapolate these totals to all ITS.gov payments in our scope. No payments that Fiscal Service disbursed through ITS.gov have been matched to the TOP database since the inception of ITS.gov in early 2004. As a result, a significant amount of delinquent debt may have gone uncollected, resulting in potential improper payments.[28] A separate audit of uncollected debt from ITS.gov disbursements would be required to determine an accurate estimate of the resulting improper payments.

Recommendation

We recommend that the Acting Commissioner of Fiscal Service:

1. Implement a control to ensure all eligible TDO payments disbursed through ITS.gov are matched against the TOP database.

[26] The IDD service facilitates payments to beneficiaries in foreign countries.

[27] Fiscal Service analyzed Social Security Administration, Department of Veterans Affairs, and Railroad Retirement Board IDD payment data from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 15, 2025. The payment data was matched against the TOP database as of December 2025 because a TOP official told us they could not match against historical TOP data for these exact periods.

[28] Improper payments, as defined by 31 U.S.C. § 3351, include overpayments. Overpayments include payments exceeding what should have been paid after offsets for any payees with debt recorded in TOP.

Management Response

Fiscal Service management concurs and plans to enhance its international payment systems in the future to enable this type of screening. Management stated they are currently unable to implement the recommendation as they do not have the technical capability to match international payments for potential offset due to the complexity of purchasing and valuing foreign currency.

OIG Comment

Fiscal Service management's planned corrective actions meet the intent of our recommendation. Management should include its planned corrective actions and expected completion date(s) in JAMES.

Finding 5 Fiscal Service Issued Improper Duplicate International Payments

Fiscal Service issued six duplicate NTDO payment schedules through ITS.gov,[29,30] resulting in nearly $300,000 in improper payments. This error occurred primarily because the NTDO official submitted these payments twice, using the same payment schedule number. Fiscal Service did not identify this issue because ITS.gov, which processes NTDO payment schedules, does not have a control to prevent duplicate payment schedule numbers from the same NTDO.

OMB Circular A-123, Appendix C, states that, to be effective, programs should not operate in a "pay-and-chase" model. Rather, programs should prioritize preventing improper payments from happening and avoid expending resources to try and recover the overpayments. Although NTDO officials are required by the Treasury Financial Manual to ensure that a payment is not a

[29] Fiscal Service does not disburse NTDO payments. Rather, NTDOs disburse international payments, which Fiscal Service issues through ITS.gov. NTDOs are responsible for adhering to the various federal laws and regulations governing disbursing official obligations.

[30] These duplicates were not discovered through our sample testing for payments issued through ITS.gov. Rather, they were discovered during our data reliability assessment while filtering data for anomalies, including apparent duplicates.

duplication prior to certification,[31] Fiscal Service should implement a control in ITS.gov to prevent duplicate schedule numbers from the same NTDO. While the NTDO subsequently recovered the payments 38 days after the payments were issued, the time needed to do so wasted federal resources.

Recommendation

We recommend that the Acting Commissioner of Fiscal Service:

1. Implement a control for ITS.gov payments to ensure that an NTDO cannot enter duplicate payment schedule numbers into ITS.gov within the same fiscal year.

Management Response

Fiscal Service management concurs with the recommendation and will implement a control for ITS.gov to prevent NTDOs from entering duplicate payment schedule numbers. Fiscal Service management stated any error resulting in an improper payment was due to the other federal agency's failure to properly verify the accuracy and legitimacy of its payment before certifying the payment to Fiscal Service for processing.

OIG Comment

Fiscal Service management's planned corrective action meets the intent of our recommendation.

While we agree that the payor agency is required to ensure the payment is not a duplicate prior to certification, Fiscal Service should implement controls to prevent improper payments involving Fiscal Service systems, as required by OMB Circular A-123, Appendix C. Management should include its planned corrective action and expected completion date in JAMES.

[31] Treasury, Financial Manual, Volume 1, Part 4A, Chapter 2000, Section 2075, *Preaudit of Vouchers* (April 9, 2025)

Finding 6 Fiscal Service Did Not Prevent PAM Disbursements That Included Clearly Invalid Payee TINs

Fiscal Service disbursed payments that included clearly invalid payee TINs. TINs are nine-digit numbers unique to each payee. TINs cannot contain letters or use the same number for all nine digits. For example, if a TIN is ABC-DE-1234 or 999-99-9999, it is clearly invalid. We reviewed payee TINs for 18 payment schedules[32] and determined that 4 (22 percent) were disbursed with clearly invalid TINs. This occurred because PAM's configuration does not detect or reject clearly invalid TINs. Based on our audit results, we asked Fiscal Service to query PAM for payments that included clearly invalid TINs for two months within our audit scope period. The query identified more than 560,000 unknown payments,[33] totaling approximately $23 billion, with clearly invalid payee TINs. Without valid TINs, we cannot determine if the payees identified in the PAM query had debt recorded in TOP and required offset. As such, the number of improper payments is unknown and would require a separate audit to determine. If only a fraction of these payments went to payees with delinquent debt, the number of potential improper payments is substantial.

The payor agency is responsible for the accuracy of payee information and for identifying whether payments are eligible for TOP, as certain types of payments are exempt from offsets; but OMB Circular A-123, Appendix C, states that all programs must proactively manage their payment integrity risk to prevent improper and unknown payments. In addition, Fiscal Service officials are required to ensure applicable delinquent debts are collected for any payments they disburse,[34] and cannot do so without valid TINs. Therefore, Fiscal Service should be proactive in mitigating the risk of improper and unknown payments. As PAM processes more than a billion payments annually, without a control to detect and reject

[32] While our testing was generally limited to internal controls at the payment schedule level, the records Fiscal Service provided for 18 of 77 PAM payments schedules from our statistical sample allowed us to see individual payment-level details, such as the payee TIN.

[33] OMB Circular A-123, Appendix C, defines unknown payments as those that an agency cannot determine to be either proper or improper because of insufficient or lack of documentation. Ninety-eight percent of the 560,000 payments originated from the Internal Revenue Service.

[34] 31 U.S.C. § 3716 and 31 CFR 285.4 and 285.5

clearly invalid TINs, Fiscal Service is at risk of disbursing a significant number of improper payments.

Recommendations

We recommend that the Acting Commissioner of Fiscal Service:

1. Implement a control to reject any payments with clearly invalid TINs and make the agencies resubmit the payments with valid TINs.

Management Response

Fiscal Service management concurs and is evaluating solutions to implement TIN verification screening functionality.

OIG Comment

Fiscal Service management's planned corrective action meets the intent of our recommendation. Management should include its planned corrective action and expected completion date in JAMES.

2. Issue guidance to agencies explaining the importance of inputting TINs accurately, and include in the guidance a requirement that agencies notify Fiscal Service of the need to use clearly invalid TINs.

Management Response

Fiscal Service management concurs and will provide guidance to agencies emphasizing the need to accurately input TINs once they have implemented a solution for TIN verification.

OIG Comment

Fiscal Service management's planned corrective action meets the intent of our recommendation. Management should include its planned corrective action and expected completion date in JAMES.

Finding 7 Fiscal Service Did Not Ensure Personnel Validated Only Complete Payment Authority Delegation and Designation Forms

Fiscal Service personnel validated incomplete payment authority delegation and designation forms because Fiscal Service does not have a supervisory control to ensure its personnel reviewed the forms properly. Payment authority delegation and designation forms enable the head of an agency to appoint responsible officials to exercise payment authority on behalf of their agency. Fiscal Service policy requires Fiscal Service personnel to review these forms to ensure they are complete before the forms are validated. However, Fiscal Service personnel validated 31 of 66 (47 percent) forms tested despite the forms being incomplete.

Some significant missing fields were effective date, training completion date, and designee signature. The effective date for delegation and designation should be determined by the agency and dictates when the individual should start their role. By validating forms without effective dates, Fiscal Service personnel, rather than agency officials, made those positions effective on the date Fiscal Service validated the forms. Related to training completion date, COs must complete training to ensure they understand and can perform their responsibilities. Without this field completed, Fiscal Service personnel do not know that the COs have completed the training and understand the requirements of their designated role. Lastly, related to designee signature, forms must be signed by the designee as it represents their acknowledgement and acceptance of their role and responsibilities for disbursing payments and expending federal funds. Therefore, it is imperative that Fiscal Service personnel ensure the forms are complete before validating them.

Recommendation

We recommend that the Acting Commissioner of Fiscal Service:

1. Implement a supervisory control to ensure Fiscal Service personnel adhere to policy and validate only complete payment authority delegation and designation forms.

Management Response

Fiscal Service management agreed and stated they implemented this recommendation by adding a new control requiring two levels of supervisory review and approval over payment authority delegation and designation forms.

OIG Comment

We have not verified Fiscal Service management's corrective action taken, but the stated corrective action meets the intent of our recommendation. Management should include its planned corrective action and expected completion date in JAMES.

Matter of Concern

There are data discrepancies between PAM and SPS payment records. We identified discrepancies in 8 of 77 (10 percent) sampled PAM payments, where values in the payment type field did not match between PAM and SPS. The SPS certification and PAM Payment Request File (PRF)[35] each contain a payment type field, but the values available for the fields do not match across systems. Specifically, PAM allows 14 payment types, which are broad payment categories, such as monthly benefit. SPS allows 27 payment types, some of which are more detailed categories, such as "OPM benefit" and "SSA benefit." Thus, the data in each system can differ, making it difficult to ensure that the payment information in an SPS certification matches the information in its corresponding PAM PRF. For example, for 2 of 8 discrepancies, the payment was categorized as a "vendor" payment type in PAM versus "miscellaneous" in SPS. Fiscal Service officials were unable to provide a clear answer for why the available payment type values do not match between systems, but the officials did not believe the differences are material. In addition, Fiscal Service officials told us that the payment type field does not affect a payment's disbursement instructions, which tell a financial institution who to pay and in what amount. While Fiscal Service officials believe that the payment type field has no impact on

[35] A PRF, also referred to as a Standard Payment Request, is defined by Fiscal Service as a file received from a federal agency containing one or more payment schedules, intended for disbursement to the agency's payees using the included payment instructions.

disbursement, it is unclear if payment type discrepancies would affect other areas, such as payment statistics.

As SPS is used by payor agencies to request payments to be disbursed through PAM and provides the legal authorization for Fiscal Service to make payments, it is prudent for Fiscal Service to minimize data discrepancies between the two systems.

* * * * * *

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss the report, you may contact me at (202) 607-7851 or Justin Walker, Audit Manager, at (202) 422-1777. Major contributors to this report are listed in appendix 3.

Gregory J. Sullivan /s/
Audit Director

Appendix 1: Objectives, Scope, and Methodology

The objectives of our audit were to (1) determine the adequacy of controls in place for granting or restricting access to the Bureau of the Fiscal Service's (Fiscal Service) sensitive payment systems; (2) determine the adequacy of controls in place to ensure payments are made in accordance with federal laws, regulations, and guidance; and (3) follow up on any allegations of improper or fraudulent payments made by Fiscal Service.

The scope of our audit included the Secure Payment System (SPS), the Payment Automation Manager (PAM), and International Treasury Services (ITS.gov). The scope period for the first objective was from October 1, 2024, through February 28, 2025. The scope period for the second objective was from December 1, 2024, through March 16, 2025.[36] The third objective regarding allegations of improper or fraudulent payments covered October 1, 2024, through March 16, 2025, as well as fiscal years 2023 and 2024. We conducted audit fieldwork from May 2025 through March 2026.

To accomplish our objectives, we reviewed applicable laws, regulations, standard operating procedures (SOPs), and guidance related to Fiscal Service payment systems, including:

- P.L. 93-579, Privacy Act of 1974 (December 31, 1974)
- Titles II and III of P.L. 107-347, E-Government Act of 2002 (December 17, 2002)
- 5 U.S.C. § 552a, *Records maintained on individuals* (October 2, 2024)
- 26 U.S.C. § 6103, *Confidentiality and disclosure of returns and return information* (January 4, 2025)

[36] The scope of our payment sample testing was December 1, 2024, through December 31, 2024, and February 15, 2025, through March 15, 2025, for ITS.gov payments; and from December 1, 2024, through December 31, 2024, and February 15, 2025, through March 16, 2025, for PAM payments. The scope period specifically related to our sampling universe for PAM payments extended an additional day because of a date field Fiscal Service used to generate the universe that was missing from the output. Because of the time and resources needed to generate a new output and reperform the data reliability assessment on new data, we used the universe as provided by Fiscal Service.

- 31 U.S.C. § 3321, *Disbursing authority in the executive branch* (July 11, 2006)
- 31 U.S.C. § 3325, *Vouchers* (July 11, 2006)
- 31 U.S.C. § 3351, *Definitions* (March 2, 2020)
- 31 U.S.C. § 3354, *Do Not Pay Initiative* (March 2, 2020)
- 31 U.S.C. § 3716, *Administrative offset* (May 9, 2014)
- 44 U.S.C. § 3301, *Definition of record* (November 26, 2014)
- 44 U.S.C. § 3303, *Lists and schedules of records to be submitted to the Archivist by head of each Government agency* (November 26, 2014)
- 31 U.S.C. § 3528, *Responsibilities and relief from liability of certifying officials* (October 19, 1998)
- 31 CFR § 1, *Disclosure of Records* (October 20, 2022)
- 31 CFR § 285, *Debt Collection Authorities Under the Debt Collection Improvement Act of 1996* (August 16, 2022)
- 36 CFR § 1222, *Creation and Maintenance of Federal Records* (December 12, 2022)
- 36 CFR § 1225, *Scheduling Records* (October 2, 2009)
- Fiscal Service, *Privacy Act of 1974; System of Records*, 85 Fed. Reg. 11776 (February 27, 2020)
- Government Accountability Office (GAO)*, Standards for Internal Control in the Federal Government* (GAO-14-704G; September 2014)
- Office of Management and Budget (OMB), Circular No. A 123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016)
- OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016)

- OMB, Circular A-123, Appendix C, *Requirements for Payment Integrity Improvement* (March 5, 2021)
- OMB, Memorandum M-19-03, "Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program" (December 10, 2018)
- National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" (Sept. 2020)
- Department of the Treasury (Treasury), Directive Publication 85-01, Volume 1, *Treasury Information Technology Security Program* (February 28, 2022)
- Treasury, Financial Manual, Volume I, Part 3, *Receivable and Delinquent Debt Management* (April 9, 2025)
- Treasury, Financial Manual, Volume I, Part 4A, *Payment-Related Activities Within the Authority Granted to the U.S. Chief Disbursing Officer (CDO)* (April 9, 2025)
- Fiscal Service, *Baseline Security Requirements* (December 18, 2024)
- Fiscal Service, *ITS.gov Payment Release SOP* (as of July 31, 2023)
- Fiscal Service, *ITS.gov NTDO Payment Processing Role Standard Operating Procedures* (as of July 1, 2023)
- Fiscal Service, *PAM Access Management Document*, Version 4.2 (May 8, 2024)
- Fiscal Service, *PAM Driver Manual,* Version 2.1 (August 15, 2017)
- Fiscal Service, *PAM Input File Specifications – Standard Payment Request,* Version 5.0.2 (June 17, 2019)
- Fiscal Service, *PAM Operations Processing Procedures* (n.d.)
- Fiscal Service, *PAM Supplementary Specification*, Version 12.1.0 (March 4, 2024)

- Fiscal Service, Policy 301-2, *Email and Instant Messaging Policy* (August 18, 2024)
- Fiscal Service, *Remove Certified Schedule/Stop Payment Request* (September 20, 2023)
- Fiscal Service, *SPS Schedule Import 440 File Format,* Version 2.4 (Feb. 2025)

We interviewed Fiscal Service personnel involved in the management of SPS, PAM, and ITS.gov and associated access and payment-related programs, including those from the Federal Disbursement Services and Enterprise Information Technology Operations Divisions.

To determine the adequacy of controls in place for granting or restricting access to SPS, PAM, and ITS.gov, we identified seven NIST SP 800-53[37] controls related to the design, implementation, and operating effectiveness of internal controls that were significant to the access process, including controls over design of control activities, separation of duties, access control policies and procedures, and access rights. We assessed whether the documented process was followed for granting or restricting user access to each system. Additionally, we assessed whether the access-related internal controls, where applicable, were properly designed, implemented, and operating effectively.

To test the design of the identified NIST SP 800-53 controls, we reviewed Treasury and Fiscal Service policies and SOPs to assess whether the documented controls achieved the objective. To test the implementation of the identified NIST SP 800-53 controls, we conducted interviews and walkthroughs with Fiscal Service personnel to ensure that the controls were implemented in SPS, PAM, and ITS.gov, as applicable. To test the operating effectiveness of the identified NIST SP 800-53 controls, we selected 21 users[38] who had access granted or removed from October 1, 2024, through February 28, 2025, for one of the following systems: (1) 4 users with access to SPS's server and

[37] We identified seven NIST SP 800-53 controls that were significant to the PAM and SPS servers and databases, and six of those controls were also applicable to the ITS.gov application.

[38] One individual had access added and removed for both PAM and SPS. As a result, we reviewed 20 unique users.

database, (2) 11 users with access to PAM's mainframe and database, and (3) 6 users with access to the ITS.gov application.

For each user that had their access granted or removed for PAM, SPS, and ITS.gov, we verified the completeness of each user's access by reviewing documentary evidence, including emails, PAM, SPS, and ITS.gov records, and records from other internal Fiscal Service systems, to determine whether (1) required Rules of Behavior forms were provided to and signed by the user; (2) the user completed security and privacy awareness training; (3) access requests were submitted by and to the appropriate officials, if applicable; (4) requests for access removal were submitted by and to the appropriate officials for all users who had left the organization; and (5) management approval for system access was documented, if applicable.

To determine the adequacy of controls in place to ensure payments are made in accordance with federal laws, regulations, and guidance, we assessed whether PAM and ITS.gov payments followed SOPs and payment-related internal controls were properly designed, implemented, and operating effectively. We identified 25 internal controls significant to the payment process, including controls over segregation of duties; authorizing, recording and documenting transactions; and the completeness, accuracy, and validity of data. We tested 6 internal controls in SPS: 3 for design and implementation; and 3 for design, implementation, and operating effectiveness. We tested 11 internal controls in PAM: 4 for design and implementation; and 7 for design, implementation, and operating effectiveness. We tested 8 internal controls in ITS.gov: 4 for design and implementation; and 4 for design, implementation, and operating effectiveness.

To test the design of internal controls, we reviewed SOPs and other documentation to determine whether the controls in SPS, PAM, and ITS.gov achieved the objective of ensuring payments are disbursed and issued in accordance with laws, regulations, and federal guidance. To test the implementation of internal controls, we conducted interviews and walkthroughs with Fiscal Service personnel and officials. During walkthroughs, Fiscal Service personnel and officials demonstrated, in a test environment, how the controls functioned at the application level in SPS, PAM, and ITS.gov. To test the operating effectiveness of internal controls, we statistically selected stratified random samples of PAM and

ITS.gov payment schedules to determine whether the controls were operating effectively in SPS, PAM, and ITS.gov.

We statistically selected a stratified random sample of 77 of 56,030 PAM payment schedules from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 16, 2025, at 90 percent confidence, assuming a 5 percent error rate and 5 percent precision. We selected random samples, proportional to the universe for those periods, from two strata: (1) 38 payment schedules from December 1, 2024, through December 31, 2024; and (2) 39 payment schedules from February 15, 2025, through March 16, 2025.

For each sample PAM payment schedule, we reviewed (1) sample payment data for accuracy and completeness by reconciling the data with PAM and SPS records; (2) SPS records to verify that the Data Entry Operator (DEO) and Certifying Officer (CO) for each payment schedule were different individuals; (3) PAM and SPS records to verify that each payment schedule was certified by a CO prior to disbursement; (4) PAM and SPS records to verify the schedule was matched against the Treasury Offset Program (TOP), if the payment schedule was designated for TOP matching; (5) ITS.gov records to verify the PAM payment schedule went through Office of Foreign Assets Control (OFAC) screening, if applicable; and (6) PAM records to verify the schedule passed validation screening.[39]

We also reviewed a query of all PAM payments from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 15, 2025, to verify that no payment schedules were disbursed without a Treasury Account Symbol (TAS)/Business Event Type Code (BETC)[40] for each payment in the schedule. For Type B bulk payments disbursed after February 14, 2025, we reviewed PAM and SPS records to determine whether each payment schedule had at least one

[39] A validation check is performed to ensure a payment schedule is in proper form, approved and certified, and computed correctly prior to disbursement.

[40] Treasury, collaborating with each agency and OMB, assigns a TAS as a code that identifies a specific fund account (for appropriations, expenditures, receipts, etc.). A BETC is a two-to-eight-character letter code that indicates the type of activity being reported, such as collection, disbursement, offsetting collection, or payment.

TAS/BETC[41] and the payment schedule passed the validation check.

We statistically selected a stratified random sample of 81 of 16,674 ITS.gov payment schedules from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 15, 2025, at 90 percent confidence, assuming a 5 percent error rate and 5 percent precision. We selected samples from eight strata proportional to the universe for those periods, ensuring at least five payment schedules were selected from each stratum. We selected 42 payment schedules from December 1, 2024, through December 31, 2024, from the following 4 strata: (1) 10 Treasury Disbursing Office (TDO), (2) 22 Non-Treasury Disbursing Office (NTDO), (3) 5 TDO International Direct Deposit (IDD), and (4) 5 NTDO IDD payment schedules. For February 15, 2025, through March 15, 2025, we selected 39 payment schedules from the following 4 strata: (5) 10 TDO, (6) 19 NTDO, (7) 5 TDO IDD, and (8) 5 NTDO IDD payment schedules.

For each sample ITS.gov payment, we reviewed (1) sample payment data for accuracy and completeness by reconciling the data with ITS.gov and SPS records, where applicable; (2) ITS.gov records to verify the ITS.gov payment schedule went through OFAC screening;[42] and (3) ITS.gov records to verify the schedule passed validation screening. For TDO and TDO IDD payment schedules, we reviewed (1) SPS records to verify that the DEO and CO for each payment schedule were different individuals, and (2) ITS.gov and SPS records to verify that each payment schedule was certified by a CO prior to disbursement. For non-IDD NTDO payment schedules, we reviewed (1) ITS.gov records to verify that the Creator and Verifier[43] for each payment schedule were different individuals, and (2) ITS.gov records to verify that each payment schedule was certified by a Verifier prior to payment issuance.

[41] Fiscal Service updated the PAM Payment Request File to require that, starting February 15, 2025, agencies include a TAS/BETC for each individual payment in a payment schedule. Because we did not test payments at the payment detail level, we verified operating effectiveness of the TAS/BETC requirement through the validation check control.

[42] NTDO IDD payment schedules are primarily processed outside of ITS.gov. The OFAC screening was the only control tested for these payment schedule types.

[43] Because NTDO payments are not disbursed by Fiscal Service, NTDO personnel are not assigned DEO and CO roles in SPS. ITS.gov has similar types of roles with different names: Creators create payment schedules in ITS.gov, and Verifiers certify the payment schedules for Fiscal Service to issue through ITS.gov.

To assess whether the DEOs and COs who created, edited, or certified PAM and ITS.gov payment schedules in SPS were authorized to perform these actions, we selected a non-statistical sample of 108 payment schedules from our statistical samples of 158 PAM and ITS.gov payment schedules. We then selected all designation forms for the DEOs and COs[44] associated with these payment schedules that were in effect from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 16, 2025. We also selected all delegation forms for the corresponding Designating Officials (DO) and Heads of Agency[45] that were in effect during the same period. We tested the forms to determine whether the DEOs and COs were designated by an authorized official from their respective agency when the associated payment schedules were created, edited, or certified, and there was a complete chain of delegations, with all required signatures, to the respective Head of Agency. We also tested the forms for completeness by determining whether all required fields were properly filled. As our selection was non-statistical, our results cannot be extrapolated to the entire population and are not representative of all DEOs, COs, and DOs. Table 1 lists the number and type of forms we tested.

Table 1: Payment Authority Forms Tested

Role	Enrollment Forms[46]	Renewal Forms[47]	Total
DEO	15	33	48
CO	13	36	49
DO	38	42	80
Total	66	111	177

Source: FS Forms 210DEO, 210CO, and 2958DO, and delegation and designation renewal forms in effect from December 1, 2024, through December 31, 2024, and from February 15, 2025, through March 16, 2025

To assess whether payment schedules were properly removed from PAM and ITS.gov, we selected all schedules submitted for processing through PAM and ITS.gov from December 1, 2024, to

[44] DEOs and COs are designated using FS Form 210DEO, "Designation for Data Entry Operator," and FS Form 210CO, "Designation for Certifying Officer," respectively.

[45] DOs are delegated payment authority using FS Form 2958DO, "Delegation of Authority."

[46] FS Forms 210DEO, 210CO, and 2958DO are referred to as "enrollment forms." These forms contain several required fields, such as the designee's information and signature, the designator or delegator's information and signature, and the effective date for the designation or delegation.

[47] A renewal form is a streamlined version of an enrollment form, containing only two required fields to be completed by the requesting agency, and is used for individuals whose designation or delegation has not expired.

March 15, 2025, that were rejected, cancelled, reversed, or otherwise not disbursed. We tested each removed payment schedule to determine whether the removal was requested by an authorized official from the agency that submitted the payment schedule, the request was approved by the appropriate Fiscal Service official, and the payment schedule was removed from the associated payment system.

To follow up on any allegations of improper or fraudulent payments made by Fiscal Service, we obtained testimonial evidence from Fiscal Service officials at the beginning of the audit, during planning, and near the close of fieldwork, regarding whether they were aware of any specific allegations of improper fraudulent or payments processed through Fiscal Service payment systems or were aware of any such allegations. When improper payments were identified during the audit, we determined the cause and the effect of the improper payment, to the extent possible, and whether there was evidence of any violation of administrative or criminal law that constituted fraud.

To assess the reliability of Fiscal Service data, we performed testing, including electronic testing, for obvious errors in accuracy and completeness; reviewed existing information about the data and the systems that produced it; and interviewed Fiscal Service agency officials knowledgeable about the data. When we found discrepancies (such as missing data or duplicate values), we brought them to the attention of Fiscal Service officials and worked with the officials to correct them. We determined that the data was sufficiently reliable for purposes of this audit.

We assessed internal controls and compliance with laws and regulations necessary to conclude on our audit objectives. We reviewed the GAO's *Standards for Internal Control in the Federal Government* (Green Book) to identify the components and principles of internal control related to the context of the audit objectives. Specifically, we determined that the Control Environment and Control Activities components, including the following principles, were significant to our audit objectives:

- Principle 3 – *Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives*.

- Principle 10 – *Management should design control activities to achieve objectives and respond to risks*.
- Principle 11 – *Management should design the entity's information system and related control activities to achieve objectives and respond to risks*.
- Principle 12 – *Management should implement control activities through policies.*[48]

We assessed management's design, implementation, and operating effectiveness of internal controls related to (1) granting or restricting access to Fiscal Service's sensitive payment systems; and (2) ensuring payments are made in accordance with federal laws, regulations, and guidance, as applicable. Because our review was limited to these aspects of internal control, our audit may not disclose all internal control weaknesses and deficiencies that may have existed at the time of this audit. The internal control weaknesses and deficiencies are discussed in the findings of this report.

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 objectives.

[48] GAO, Green Book, pp. 27, 45, 51, and 56

Appendix 2: Management Response

May 29, 2026

Gregory J. Sullivan
Audit Director, Anti-Money Laundering,
Terrorist Financing, Intelligence, and International Programs
Office of Inspector General
U.S. Department of the Treasury
875 15th Street, N.W.
Washington, D.C. 20005

Dear Mr. Sullivan:

Thank you for the opportunity to review the Office of Inspector General's (OIG) draft report entitled *Fiscal Service's Sensitive Payment Systems' Controls are Generally Adequate but Weaknesses and Deficiencies Exist* (Draft Report). The U.S. Department of the Treasury (Treasury) values OIG's analysis and has provided technical comments under separate cover.

The Draft Report examines the Bureau of the Fiscal Service's (BFS) controls regarding access to its sensitive payment systems and payments made through those systems. As the Draft Report acknowledges, BFS has robust controls regarding each of these areas, and those controls—after extensive testing from OIG over eleven months of fieldwork—have proven to be generally adequate.

BFS agrees with the goals underpinning OIG's nine recommendations, two of which BFS has already implemented. Specifically, OIG's first recommendation calls for BFS to update its policies to include procedures for modifying users' access to the Payment Automation Manager (PAM) database. BFS has already implemented this recommendation by migrating the PAM database off the mainframe and has modernized and standardized its access control procedures through the implementation of a new enterprise-level standard operating procedure that applies to all database platforms. OIG's ninth recommendation calls for BFS to implement supervisory controls to ensure that personnel validate only complete payment authority delegation and designation forms. In response, BFS has implemented a new control requiring two levels of supervisory review and approval over such forms.

OIG's second recommendation addresses the unique situation of a Treasury employee – not a BFS employee – being granted access to Fiscal Service payment systems prior to signing a Rules of Behavior form, and recommends that BFS ensure all users sign such a form prior to being granted access. BFS agrees and will update its policies to explicitly state that the Rules of Behavior apply to all users, regardless of employer, who access any BFS data and will require either a signed form or system-verified completion of the Rules of Behavior training module prior to gaining access to BFS systems.

The third and fourth recommendations call for BFS to evaluate its Data Loss Prevention configurations to determine whether additional controls are necessary to mitigate the risk of external transmission of low-risk Personally Identifiable Information (PII), and to update BFS policies to clarify when low-risk PII constitutes Controlled Unclassified Information. BFS concurs with each of these recommendations and will implement them.

OIG also recommends that BFS implement a control to ensure that international payments are matched against the Treasury Offset Program database. BFS agrees with the goal of this recommendation but is unable to implement it at this time. Agencies may submit international payment requests to BFS in foreign currencies, while benefit payments are submitted in U.S. dollars with foreign exchange occurring at the time of disbursement. Because of the complexity of valuing the purchase of foreign currency at a particular date and time, we currently do not have the technical capability to match such payments for potential offset. BFS intends to implement enhancements to its international payment systems in the future to enable this type of screening.

The sixth recommendation calls for BFS to implement controls to prevent other agencies from using duplicate payment schedule numbers for their international payments within the same fiscal year. BFS disagrees with the underlying finding because any error resulting in an improper payment was due to the other federal agency's failure to properly verify the accuracy and legitimacy of its payment before certifying the payment to BFS for processing. Nonetheless, BFS will implement the recommendation.

BFS agrees with the seventh and eighth recommendations to implement controls to reject payments with invalid Taxpayer Identification Numbers (TINs) and issue guidance to agencies regarding the importance of inputting TINs accurately. We are evaluating solutions to implement initial TIN verification screening functionality. When such solutions are implemented, we will provide prior notification to agencies regarding such screening and guidance emphasizing the need to accurately input TINs.

BFS appreciates OIG's work assessing our sensitive payment systems controls. Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

Sincerely,

Joseph Gioeli
Acting Commissioner
Bureau of the Fiscal Service

The Department of the Treasury

Appendix 3: Major Contributors to This Report

Justin Walker, Audit Manager
Andrew Clements, Audit Manager
Mitul Patel, Audit Manager
Laura Miller, Auditor-in-Charge
Crisman Jones, Auditor
Andrew Malcolm, Auditor
Jung Hyub Lee, IT Specialist
Alberto Garza, Data Reliability Specialist
Herb Addy, Referencer

Appendix 4: Report Distribution

Department of the Treasury

Secretary
Deputy Secretary
Acting Fiscal Assistant Secretary
Office of Strategic Planning and Performance Improvement
Office of the Deputy Chief Financial Officer, Risk and Control Group

Bureau of the Fiscal Service

Acting Commissioner
Office of Inspector General Audit Liaison

Office of Management and Budget

Office of Inspector General Budget Examiner

U.S. Senate

Chairman and Ranking Member
Committee on Banking, Housing, and Urban Affairs

Chairman and Ranking Member
Committee on Finance

Chairman and Ranking Member
Committee on Homeland Security and Governmental Affairs

U.S. House of Representatives

Chairman and Ranking Member
Committee on Financial Services

Chairman and Ranking Member
Committee on Oversight and Government Reform

Chairman and Ranking Member
Committee on Ways and Means

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/