Department of Health and Human Services
Office of Inspector General
Office of Audit Services

June 2025 | A-18-24-03700

HHS's Grant Payment System Lacked Effective Internal Controls To Prevent $7.8 Million in Fraud, and HHS Has Begun Taking Corrective Actions To Reduce Fraud Risk

REPORT HIGHLIGHTS

June 2025 | A-18-24-03700

HHS's Grant Payment System Lacked Effective Internal Controls To Prevent $7.8 Million in Fraud, and HHS Has Begun Taking Corrective Actions To Reduce Fraud Risk

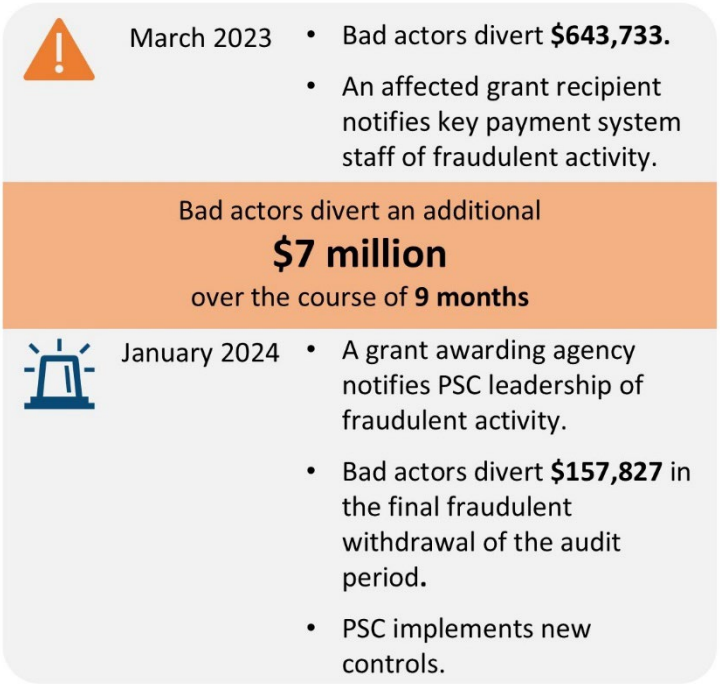
Why OIG Did This Audit

- From March 2023 through January 2024, bad actors fraudulently diverted $7.8 million in grant funds from HHS's Program Support Center (PSC) grant payment system.
- Bad actors were able to gain access to the PSC grant payment system by masquerading as grant recipients and requesting account changes, including changes to grant recipients' banking information.
- This audit reviewed PSC's internal controls, risk management, and cybersecurity controls over the PSC grant payment system to determine whether the system was properly protected.

What OIG Found

- At the time of the fraud, PSC did not have effective internal controls to communicate fraudulent activity to PSC leadership, grant awarding agencies, and grant recipients.
- PSC's approach to risk management was siloed and did not address the risk of bad actors gaining access to the payment system.
- PSC did not implement some required cybersecurity controls, including mitigating weaknesses timely and conducting required IT system vulnerability scans, reviews, and approvals.

PSC has begun to take steps to mitigate the future risk of fraud.



What OIG Recommends

We made six recommendations to improve PSC's controls over its grant payment system, including that it implement additional cybersecurity controls, finalize and implement bank account verification processes, and develop standard operating procedures.

PSC concurred with all six of our recommendations.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

From March 2023 through January 2024, bad actors fraudulently diverted a total of $7.8 million from the Department of Health and Human Services' (HHS's) Program Support Center (PSC) grant payment system, known as the Payment Management System (Payment System). This fraudulent activity impacted 10 grants awarded to 7 HHS recipients.

The bad actors gained access to PSC's Payment System by using fake grant recipient email addresses to request access. Once they gained access, the bad actors masqueraded as grant recipients and requested account changes such as deleting valid users and changing bank accounts and other account contact information. After the bad actors made account changes, they either requested grant payments be disbursed to the changed bank accounts in their name or waited for a grant recipient to request a grant payment, which was diverted to the bad actor's bank account. These incidents led to over $10 million in grant funding being diverted to the bad actors' bank accounts. After banks rejected over $2 million of these deposits, HHS experienced an actual loss of $7.8 million in grant funds.

We performed this audit to assess internal and cybersecurity controls and information technology (IT) risk management for the Payment System and its associated business processes.

OBJECTIVE

Our objectives were to determine whether PSC: (1) designed and implemented effective internal controls, including policies and procedures, to prevent fraudulent transactions; (2) conducted adequate IT system risk management to protect its financial management systems; and (3) implemented cybersecurity controls to protect the Payment System.

BACKGROUND

Program Support Center

PSC, a component of HHS's Office of the Assistant Secretary for Administration, is a shared services organization that provides services and products to support financial management, occupational health, real estate, logistics, and operations.

Within PSC, the Payment Management Services branch processes grant payments for the Federal Government. The Payment Management Services branch acts as a fiscal intermediary between awarding agencies and recipients, providing centralized electronic payment and grant accounting support services for HHS and other federal agencies. Within this report, the term

"PSC leadership" refers to the PSC Director and the Director of the PSC Financial Management Portfolio.[1]

The Payment System

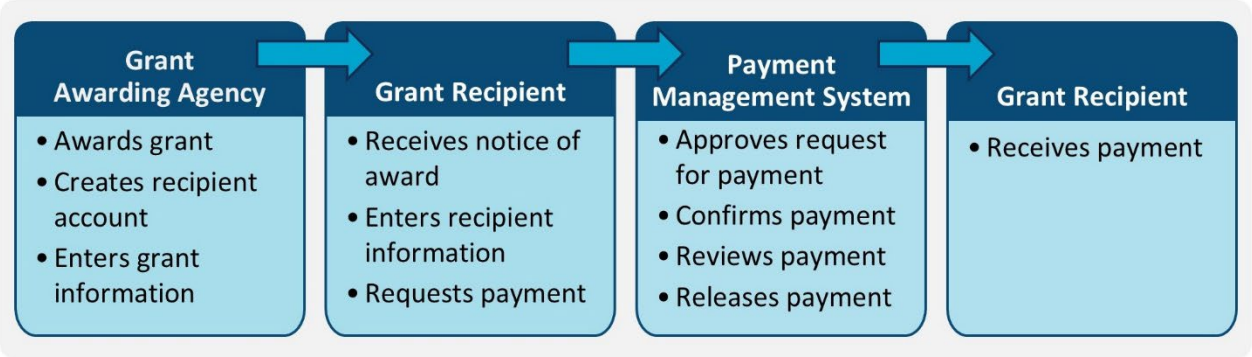
The Payment System is one of the most widely used grants payment systems in the Federal Government. In 2023, the Payment System processed over 499,000 transactions totaling over $860 billion. From October 2023 through September 2024, approximately 28 percent of the total transactions were for non-HHS grants.

The main purpose of the Payment System is to serve as the fiscal intermediary between grant awarding agencies and grant recipients. The Payment System provides grant payment and cash management services to all HHS agencies and several non-HHS agencies on a fee-for-service basis. The Payment System expedites the flow of cash between the Federal Government and grant recipients. It records award authorizations initiated by grant awarding agencies, processes grant recipient requests for funds, transmits recipient disbursement data to the awarding agencies, and manages cash flow advances to grant recipients. The Payment System is fully automated to receive payment requests, edit payments for accuracy and content, transmit payments to either the Federal Reserve Bank or the Department of the Treasury for deposit into grant recipients' bank accounts, and record the payment transactions to the appropriate accounts.

A grant recipient requests grant payments and changes to bank account information within the Payment System. Payment Management Services staff approve, confirm, and review all requests by calling and sending email notifications to the grant recipient's primary point of contact to verify the legitimacy of the system access or bank account information request. After requests are approved, confirmed, and reviewed, the Payment System releases the payment to the grant recipient. Figure 1 on the next page shows the responsibilities of a grant awarding agency and a grant recipient.

[1] The Program Support Center supports three business areas: (1) financial management; (2) occupational health; and (3) real estate, logistics, and operations. Accounting, payment management, cost allocation, and financial reporting services are included within the financial management business area of PSC.

Figure 1: Grant Payment Responsibilities



Risk Management and Internal Control Requirements

Under the authority of the Federal Managers' Financial Integrity Act, the Office of Management and Budget (OMB) requires agencies to integrate risk management and internal control functions in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. *Standards for Internal Control in the Federal Government* (Green Book), published by the Government Accountability Office (GAO), requires managers to establish an internal control environment conducive to assessing risks and implementing mitigating controls. To help managers combat fraud and preserve integrity in Government agencies and programs, GAO developed *A Framework for Managing Fraud Risks in Federal Programs.* The framework identifies control activities to prevent, detect, and respond to fraud, with an emphasis on prevention.[2]

The Federal Information Security Modernization Act established that the National Institute of Standards and Technology (NIST) is the statutory body responsible for developing information security standards and guidelines. Responsibilities include defining minimum requirements for Federal information systems and providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

Appendix B contains the Federal requirements referenced in this report.

HOW WE CONDUCTED THIS AUDIT

We reviewed Payment System controls in place from March 1, 2023, through March 31, 2024, and Payment System account payment details for the identified fraudulent transactions, which occurred between those dates. To accomplish our first objective, we examined the internal

[2] GAO identified leading practices for managing fraud risks and organized them into *A Framework for Managing Fraud Risks in Federal Programs*, which calls for a commitment "to combating fraud by creating an organizational culture and structure conducive to fraud risk management." GAO acknowledged that implementing a risk-based approach to addressing potential fraud poses a unique set of challenges for Federal managers and designed a process to ensure managers implement a holistic plan to combat fraud.

controls in place pre- and post-fraudulent activity within business processes and the information system. We reviewed Payment Management Services' policies and procedures related to entity registration, payment processes, bank account setup, and system user setup for the Payment System. To accomplish our second objective, we reviewed PSC's information system level risk assessments for the PSC financial management systems, including the Payment System. To accomplish our third objective, we reviewed HHS, OMB, and Payment System policies, standards, procedures, and guidance related to the grant payment process and the protection of the Payment System. For all three objectives, we interviewed PSC personnel, grants officers of affected grants, and relevant HHS Office of the Chief Information Officer personnel.

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.

Appendix A describes our audit scope and methodology.

FINDINGS

Before March 2023, PSC did not design and implement effective internal controls, including policies and procedures, to prevent fraudulent transactions. In addition, PSC did not conduct adequate risk management and implement all required cybersecurity controls to protect the Payment System.

Specifically, PSC had not implemented effective internal controls to communicate fraudulent activity to stakeholders timely. Further, PSC's risk management related to its business practices and information systems did not assess the risk of fraud. Finally, PSC did not implement some required cybersecurity controls, including conducting required tests, reviews, and approvals, and performing timely mitigation of identified system weaknesses. Our review of PSC personnel's compliance with cybersecurity training requirements did not result in a reportable finding.

The internal control weaknesses occurred because PSC's control environment did not facilitate fraud mitigation and did not incorporate sufficient oversight. In addition, PSC also had high vacancy and turnover rates that hindered its ability to effectively implement some manual controls.

Since the fraudulent activity was discovered, PSC has initiated some corrective actions and begun to take steps to address workforce planning issues. Although PSC is making improvements, PSC's oversight, risk management, and mitigating controls protecting the Payment System need further strengthening.

THE PROGRAM SUPPORT CENTER'S FRAUD RESPONSE WAS DELAYED BECAUSE THE PROGRAM SUPPORT CENTER DID NOT DESIGN AND IMPLEMENT CONTROLS FOR COMMUNICATING FRAUDULENT WITHDRAWALS TO INTERNAL AND EXTERNAL STAKEHOLDERS

Principle 12 of the Green Book states that management is responsible for documenting in policies each unit's responsibilities for an operational process's: (1) objectives and related risks, and (2) control activity design, implementation, and operating effectiveness (Green Book Attribute 12.03).

Principles 13 through 15 of the Green Book specify methods of internal and external communication that management should consider. Internally, information should be communicated down, across, up, and around reporting lines to all levels of the entity to enable personnel to achieve objectives, address risks, and support the internal control system. To ensure consistency, these processes should be documented as stated in Principle 12. Without appropriate communication, fraud response is likely to be delayed, and breakdowns in operating effectiveness can be expected.

PSC did not design and implement internal controls to escalate and disseminate information on fraudulent activity in the Payment System to PSC leadership, grant awarding agencies, and grant recipients. As a result, the Payment Management Services Director did not inform PSC leadership when notified of the initial series of fraudulent withdrawals in March 2023. Even after additional fraudulent withdrawals occurred and were detected from August through December 2023, the Payment Management Services Director did not inform PSC leadership.[3]

Because the March 28, 2023, fraudulent withdrawal was not communicated to PSC leadership until January 2024, PSC leadership was not aware of the need to take action to mitigate the likelihood of additional fraudulent withdrawals. Fraudulent withdrawals continued undeterred for over 9 months. At the time the fraudulent activity was first reported, bad actors had withdrawn $643,733; by the time PSC leadership was informed, the bad actors had withdrawn nearly $7 million more.

After the first fraudulent withdrawal was reported to the Payment Management Services Director by an affected grant recipient on March 28, 2023, the Director reported the incident to the Payment System Information System Security Officer (ISSO).[4] On April 5, 2023, the ISSO determined that the fraudulent activity was a non-cyber incident and therefore beyond the scope of the ISSO's responsibilities. After that determination, the Payment Management Services Director reported the incident to the HHS Office of Inspector General (HHS-OIG) and

[3] The Payment Management Services Director at the time of the fraudulent activity resigned from the position on June 14, 2024.

[4] The ISSO is tasked with maintaining the appropriate operational security posture for the IT system and is not responsible for business operations security. It is unknown when or how the Director notified the ISSO of the fraud incident.

informed the affected grant recipient that the incident had been reported to HHS-OIG. The Payment Management Services Director did not notify PSC leadership. Instead, PSC leadership was eventually notified of the fraudulent activity on January 3, 2024, over 9 months after the initial fraudulent withdrawal. However, this notification came from a grant awarding agency and not Payment Management Services.[5]

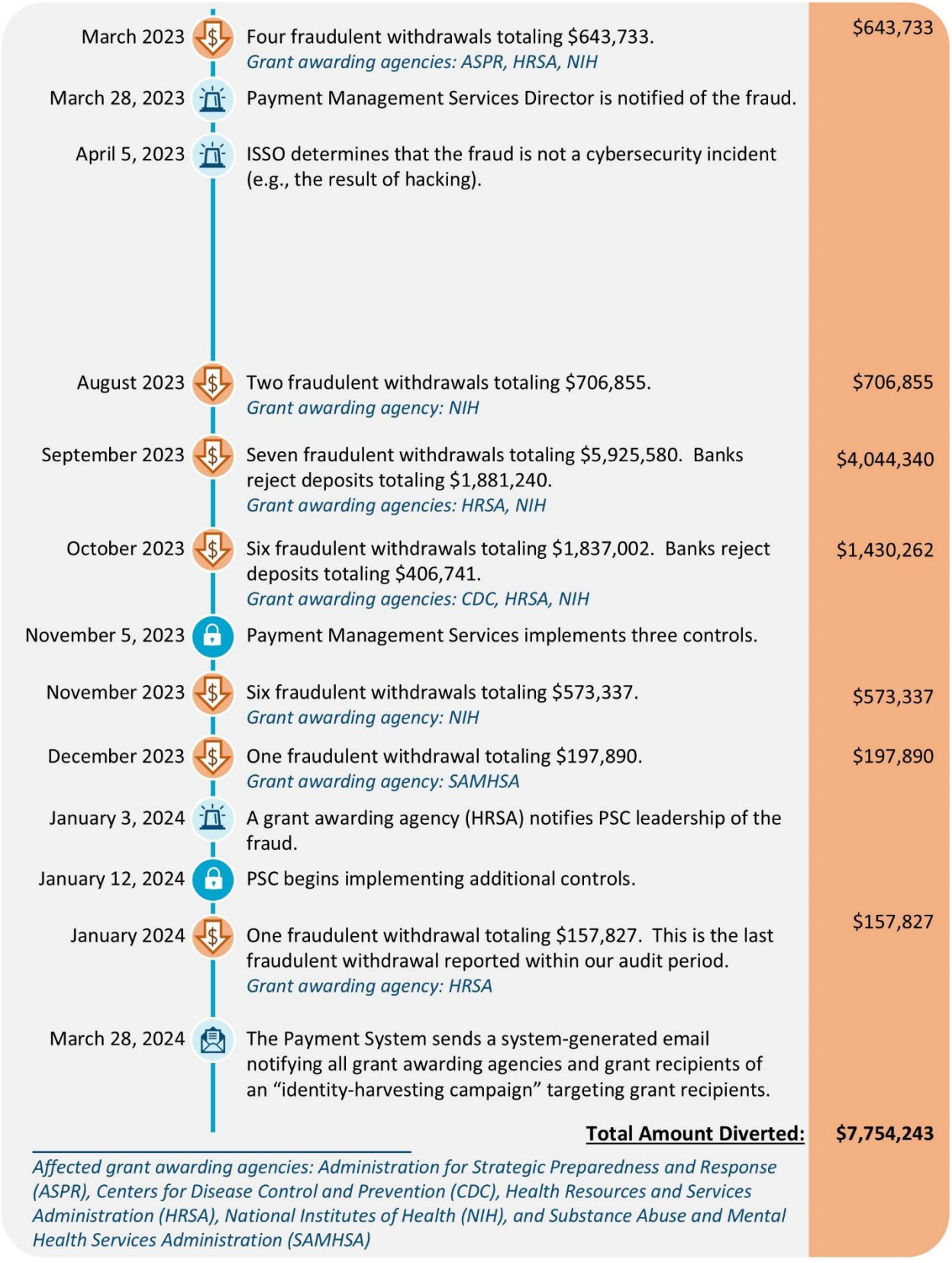
On February 9, 2024, PSC used the Payment System to send a system-generated email to grant awarding agencies and grant recipients notifying them that, in response to recent incidents of fraudulent activity, PSC was changing its login process. Additionally, on March 28, 2024, 1 year after the initial fraudulent activity was first reported, PSC used the Payment System to send a system-generated email to grant awarding agencies and grant recipients notifying them that an "identity-harvesting campaign" had been waged against grant recipients. These email communications did not: (1) refer to any specific incidents, (2) ask users to examine their individual grant accounts to verify accuracy, or (3) ask users to contact Payment Management Services if any inaccurate account information was identified. Notifying stakeholders and customers of risks and the opportunities to mitigate those risks as quickly as is feasible should be a primary action for fraud management within an organization. The emails would have been more effective had they provided additional details regarding the fraud activity to all Payment System customers and asked them to verify their account information.

Payment Management Services staff noted that, after they learned of the fraudulent withdrawals, they updated the Payment System IT Contingency Plan to require an emailed notification to HHS-OIG in the event of grant-related fraudulent activity. However, the plan update did not address the need to communicate such activity to PSC leadership or the grant community. In addition, the IT Contingency Plan details the plans and procedures for resuming Payment System operations after a service disruption or disaster and would not necessarily be activated if the fraud does not result in service disruption. Accordingly, Payment Management Services staff should have written plans for communicating potential fraud and actions to take outside of the IT Contingency Plan.

See Figure 2 on the next page for a timeline of the fraudulent activity and reporting events.

[5] The notification of fraudulent activity came from the Health Resources and Services Administration Chief Operating Officer.

Figure 2: Timeline of Fraudulent Withdrawals and Reporting Events



THE PROGRAM SUPPORT CENTER DID NOT HAVE EFFECTIVE CONTROLS TO PREVENT FRAUDULENT ACCESS TO PAYMENT SYSTEM GRANT ACCOUNTS BUT HAS SINCE MADE IMPROVEMENTS

Federal Requirements

The Green Book, in Principle 10, states that management should design control activities to achieve objectives and respond to risks. Those include entity-level control activities, transaction control activities, or both depending on the level of precision needed. As a transaction control, the Department of Health and Human Services Program Support Center Payment System Bank Information Setup and Maintenance Standard Operating Procedure states that grant recipients are responsible for adding or updating bank account information using required forms and supporting documentation.

The Program Support Center Did Not Have Effective Controls To Prevent Bad Actors From Gaining Access to Payment System Grant Accounts

At the time of the fraudulent activity, PSC did not have effective controls to prevent bad actors from gaining access to Payment System grant accounts and making changes to bank account information.

When the fraudulent withdrawals occurred, Payment System staff approving bank account changes were only required to perform limited verification procedures and were not required to contact grant recipient personnel when changes were requested. Further, once Payment Management Services staff completed bank account information changes, the Payment System was updated, and an email confirmation was sent only to the individual requesting the change. The requestors, in these cases, were the bad actors. The Payment System did not contain a grant recipient point of contact designated to verify and authorize bank account information changes.

Before the fraudulent activity, when completing annual risk assessments, PSC did not emphasize mitigating external threats. This lack of consideration resulted in the ineffective controls that allowed external individuals to circumvent the limited controls in place and gain access to some grant recipient accounts. Bad actors were able to gain access to the Payment System by pretending to be new grant recipient users and making Payment System online requests for system access. PSC did not have a process to confirm new users with already confirmed grant recipient personnel-.

Because PSC did not have effective controls to prevent bad actors from getting access to the Payment System, bad actors were able to successfully request changes to some grant recipient bank account information, including deleting valid users and changing bank accounts. Once the bank account information was changed, payments were deposited into the bad actors' bank accounts, resulting in Federal grant funds being diverted from HHS programs intended to advance the health and well-being of the people they serve.

The Program Support Center Has Begun To Implement Additional Controls and Strengthen Existing Controls To Mitigate Fraud Risk

Beginning on November 5, 2023, in response to the fraudulent activity, PSC implemented additional processes and strengthened existing controls for new user access and for changes to existing bank account information in the Payment System. Specifically, PSC implemented additional automated and manual controls for granting new user access.

Further, on January 12, 2024, PSC incorporated a manual verification procedure for confirming new grant recipient account user requests. The new procedure required multiple Payment System officials to verify and document a request for a new account user. In June 2024, PSC discontinued this manual process and replaced it with a requirement for new users to create an account with ID.me to request access to the Payment System.[6]

On February 1, 2024, PSC implemented a verification procedure for confirming whether requests for changes to bank account information, including changes to routing information, were submitted by authorized grant recipient users. Similar to the new account user verification, this procedure requires Payment System personnel to use a layered approval and verification process. The new bank account information is released to the Payment Management Services accounting and reports branch after verification. The accounting and reports personnel further review the information and release the new bank account information to update in the Payment System. Finally, the Payment System sends a confirmation to the requestor, and the Payment System dashboard updates the task status to "completed." This procedure is still in place.

In April 2024, PSC implemented other procedures, including adding new Payment System fields requiring a grant awarding agency to provide the official grant recipient's contact information when registering the recipient in the Payment System. Further, bank account information previously visible to individuals within the Payment System is now masked. Finally, PSC is working with the Department of the Treasury to develop new bank account verification processes for U.S. bank accounts. This bank account verification will be used for both grant recipient account users accessing the Payment System for the first time as well as for bank account changes made to established grant accounts.

THE PROGRAM SUPPORT CENTER'S RISK MANAGEMENT WAS SILOED

Overarching Federal Requirements for Risk Management

NIST states that organizations should establish a risk management strategy. NIST Special Publication (SP) 800-39 section 2.3.1 states that risk management requires organizations to frame, assess, respond to, and monitor risk. The Green Book states that management should

[6] ID.me is a commercial online platform that verifies an individual's identity.

identify, analyze, and respond to risks. Risk assessment provides the basis for developing appropriate risk responses.

The Program Support Center's Risk Assessment for Its Business Process Did Not Address the Risk of Fraud and the Misappropriation of Funds

The Green Book states that management should consider the potential for fraud when identifying, analyzing, and responding to risks (Green Book paragraph 8.01). Specifically, the Green Book states that the attributes that contribute to the design, implementation, and operating effectiveness of fraud risk assessment are: (1) types of fraud, (2) fraud risk factors, and (3) response to fraud risks. Paragraph 8.02 further states that, to provide a basis for identifying fraud risks, management should consider the types of fraud, including misappropriation of assets, that can occur within the entity.

PSC's risk assessments of the Payment System were not adequate because they did not include an assessment of threats from external sources or the risk of grant funds being misappropriated. Payment Management Services staff only considered the risk of fraud from internal personnel such as Payment System users. Specifically, staff indicated that they believed some users' security protocols created risk. However, staff concerns were based on anecdotal evidence, not risk assessments, and they did not consider the risk of fraud from an external actor. Further, Payment Management Services staff could not provide evidence that they had a process for identifying risks related to the misappropriation of funds.

Because it did not assess threats from external sources or the risk of grant recipient funds being misappropriated, PSC missed opportunities to establish effective controls that could have identified the bad actors who gained access to the Payment System and withdrew $7.8 million. Further, PSC was not well positioned to immediately address threats that could result in the misappropriation of grant funds.

PSC stated that it has taken fraud prevention steps to better protect against the risk of fraud from external threats, including:

- conducting machine learning scans for known anomalies and emergent threat trends,
- implementing automated individual and entity registration validation, and
- identity proofing over 30,000 worldwide grant recipients that rely on the Payment System for payment disbursements.[7]

[7] Identity proofing is the process of verifying an applicant's identity by authenticating the identity source documents the applicant provides.

The Program Support Center Did Not Use an Organization-Wide Approach to Information Technology Risk Management

NIST SP 800-39, *Managing Information Security Risk*, requires the integration of risk management processes throughout the organization, using a three-tiered approach that addresses risk at the organization level, business process level, and information system level.

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, requires organizations to perform specific tasks when preparing and conducting an information system level risk assessment. The tasks include identifying specific assumptions, constraints, threat sources, threat events, and organization vulnerabilities. The organization must also determine information security risks as a combination of the likelihood of threats exploiting vulnerabilities and the impact of such exploitation.

In addition, NIST SP 800-53, Revision 5, RA-3, requires that organizations conduct information system risk assessments that integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives. RA-3 also states that risk assessments should consider threats; vulnerabilities; likelihood; and impact to organizational operations and assets, individuals, other organizations, and the Nation. Further, risk assessments should consider risk from external parties, including individuals who access organizational systems.

PSC's IT risk management process was siloed in that it considered only IT system risks and did not consider operational or business process risks. The information system level risk assessments for all PSC financial management systems, including the Payment System, did not demonstrate a comprehensive organization-wide awareness of non-IT risks that may impact IT financial systems. Specifically, the information gathering and threat identification components of PSC's IT risk management did not take into account operational and business process risks, such as the "spoofing" that took place. The Payment System's information system level risk assessment was limited to those risks derived from a security control assessment. Although the IT system's security control assessments provide value to the risk management process, they do not provide a comprehensive view of the non-IT risks to the system. The IT risk management process did not consider potential threats from relevant organizational and business processes to establish a more comprehensive view of system risks. In addition, the Payment System IT risk assessment completed in March 2021 did not identify the lack of required multi-factor authentication control as a risk.

We also determined that none of the information system level risk assessments for PSC financial management systems included one of the tasks required by NIST for preparing and conducting the risk assessment.[8] That is, PSC did not identify the specific assumptions and

[8] See Appendix B, NIST SP 800-30, *Guide for Conducting Risk Assessments*, for a list of required tasks.

constraints under which the risk assessments were conducted. For example, PSC did not recognize that fraud was a risk that was not being assessed.

As a result, PSC did not identify fraud risks and implement mitigation controls to protect against fraudulent activity. Such mitigation controls, if implemented properly, might have removed the weaknesses that bad actors exploited, leading to the loss of $7.8 million in grant funds.

THE PROGRAM SUPPORT CENTER DID NOT IMPLEMENT CERTAIN CYBERSECURITY CONTROLS TO PROTECT THE PAYMENT SYSTEM

PSC did not implement some required cybersecurity controls, including conducting required tests, reviews, and approvals, and performing timely mitigation of identified system weaknesses. These control activities are intended to ensure the confidentiality, integrity, and availability of the Payment System.

The Program Support Center Did Not Conduct Required Cybersecurity System Controls Tests, Reviews, and Approvals

NIST SP 800-53, Revision 5; the HHS Policy for Information Security and Privacy Protection (HHS IS2P); and the HHS Office of Information Security High Value Asset Program Policy require PSC to implement credentialed vulnerability scans of the Payment System.[9] Further, NIST SP 800-53, Revision 5, and HHS IS2P both state that connectivity between an internal organization's system and an external system must be documented in an interconnection agreement, reviewed, approved, and updated according to a predefined frequency. The Payment System's System Security Plan (SSP) requires the performance of biannual penetration testing and annual review and approval of all interconnection security agreements.[10] The annual review is intended to ensure external systems continue to meet security requirements, to include having an active authorization to operate.[11] HHS policy requires interconnected Federal systems to have a current system authorization to operate.

NIST SP 800-53, Revision 5, and HHS IS2P both require cybersecurity system controls reviews to: (1) identify unnecessary and nonsecure functions, ports, protocols, software, and services; (2) review and approve the system's configuration management plan; and (3) document an inventory of system components that accurately reflects the system. Additionally, the Payment System SSP states that functions, ports, and protocols must be reviewed annually as part of the annual Payment System security assessment, and changes must go through the Payment

[9] A credentialed vulnerability scan uses authenticated user credentials that: (1) can perform functions that ordinary users are not authorized to perform or (2) have privileges that ordinary users do not have.

[10] Interconnection security agreements regulate security-relevant aspects of an intended connection between an agency and an external system that operate under two different authorities.

[11] An authorization to operate is the official management decision made by a senior organizational official or officials to authorize operation of an IT system and to explicitly accept the risk to organizational operations based on the implementation of an agreed-upon set of security and privacy controls.

System's Change Control Board. The Payment System's configuration management plan further states that all system changes are formally proposed, reviewed, and approved by the Change Control Board and requested through the automated service ticketing system. HHS IS2P requires PSC to log events that are significant and relevant to the security of the system. Event logging helps identify security incidents, policy violations, fraudulent activity, and operational problems.

While PSC implemented certain cybersecurity controls, it did not:

- perform biannual penetration testing of the Payment System;
- perform credentialed vulnerability scans of the Payment System;
- perform an annual review of the interconnection security agreements for 5 of the 10 systems authorized to access the Payment System for the purposes of creating, receiving, or transferring financial information and files with the Payment System;
- perform an annual review of configuration settings to determine whether there are any unnecessary and unauthorized information system communication ports and protocols, services, and application program interfaces connecting or exchanging information with the Payment System;
- perform weekly scans to identify unauthorized hardware, software, or firmware components within the Payment System;
- approve, in accordance with its change management process, changes to 12 firewall rules that allow network access to the Payment System; and
- conduct weekly reviews of system user activity audit logs to detect aberrant behavior such as excessive user logons and logoffs, unauthorized account creation, and privilege modifications that may indicate an active cyber threat or attack.

In addition, PSC did not include in the inventory covered by the hosting service provider's agreement two Payment System production servers that required special attention to security. These two production servers should have been included in the inventory because PSC had identified them as requiring special attention to security due to the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of the information on those servers. A complete and accurate inventory is required to be included in the agreement to ensure that the responsible IT personnel know the scope of the servers they are responsible for operating and maintaining to prevent system failures or other issues. The two identified servers were at an increased risk of not being properly managed. Further, five systems had expired system authorizations.

PSC's ability to detect and minimize threats or actual attacks was reduced when required vulnerability scans, regular cybersecurity system controls reviews, and approvals for the

Payment System were not performed. Unmitigated security risks in the Payment System could also result in bad actors migrating to and exploiting other systems connected to the Payment System to potentially steal or destroy the other systems' data.

The Program Support Center Did Not Mitigate Weaknesses Within the Required Timeframes

NIST SP 800-53, Revision 5, and HHS IS2P require the organization to correct system flaws. The Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 19-02 provides the required timeframe for remediating vulnerabilities, and the Payment System SSP states that any vulnerability discovered during Payment System scans must be addressed in the time allotted based on the severity of the finding. The HHS Standard for Plan of Action and Milestones (POA&M) requires a policy waiver for any mitigation that exceeds the required timeframe by more than 6 months. According to HHS IS2P, only authorized senior officials with the authority to formally assume responsibility and accountability for the system can accept the information security risk to operations and assets by signing the policy waiver.

HHS uses a POA&M to record information system weaknesses and identify, assess, prioritize, and monitor the progress of corrective efforts. POA&Ms are open until the weaknesses are mitigated and closed. "Funding availability" is a required element of a POA&M, and personnel are required to include information such as the type of funding (current, new, or reallocated) needed for mitigation.

As of July 25, 2024, PSC had created POA&Ms for 54 Payment System weaknesses, of which:

- none included a determination of funding availability; and
- 20 did not include the risk level/severity of the weakness, the scheduled completion date, specific actions necessary to remediate the weakness, and the source from which the weakness was identified.

Further, the corrective actions to mitigate the 31 weaknesses documented in POA&Ms and identified in a vulnerability scan were not implemented within the required remediation timeframes.

See the Table on the next page for more information about the 31 weaknesses not mitigated within required timeframes.

Table: Mitigation Exceeding Remediation Timeframes as of July 25, 2024

Risk Level/ Severity	Number of Weaknesses Not Mitigated Timely	Required Timeframe for Remediation	Number of Days Mitigation Exceeded Required Timeframe for Remediation
Critical	1	15 days	100 days
High	2	30 days	175 days
Moderate	4	90 days	1,430 days
Low	24	365 days	567 days

In addition, for 1 of the 31 weaknesses not mitigated timely, PSC did not obtain an approved waiver for the mitigation that exceeded the required timeframe by more than 6 months. Further, the senior official who reviewed and approved a waiver for the Payment System was neither the senior official who granted the Payment System's authority to operate nor the designated system owner for the Payment System.

All of these weaknesses, including the low-risk-level weaknesses, could potentially result in the disclosure of sensitive information or be used to access sensitive information, transfer funds, and change user email addresses. When remediation is not conducted timely, it leaves open a known vulnerability that can be exploited by bad actors who typically seek out vulnerable systems to attack. Additionally, when a POA&M is not properly documented with all required information, its effectiveness as a management tool is reduced. A complete POA&M is meant to inform decisionmakers and help them plan for program and process improvement.

THE PROGRAM SUPPORT CENTER CONTROL ENVIRONMENT DID NOT FACILITATE FRAUD MITIGATION

PSC did not have a control environment, the foundation for an internal control system, that facilitated fraud mitigation at the time the fraudulent activity took place. PSC's oversight was insufficient to ensure that its staff followed manual verification controls and that its risk management process was adequate. Further, PSC did not conduct oversight to enforce compliance with requirements for IT system vulnerability scans, cybersecurity controls reviews, and weakness mitigation.

At the time of the fraudulent activity, PSC also had staffing challenges that hindered its ability to effectively implement some controls. At the time, PSC relied on manual controls that required trained individuals to implement. However, high vacancy and staff turnover rates meant that there was a shortage of personnel to enact the controls.

PSC's lack of oversight combined with high vacancy and staff turnover rates led to a control environment that left the PSC vulnerable to fraud.

CONCLUSION

PSC was vulnerable to fraud because its control environment was not conducive to implementing mitigating internal controls to protect the Payment System. Bad actors exploited ineffective controls to successfully access and withdraw grant funds from the Payment System. Due to ineffective controls, bad actors were able to fraudulently withdraw grant funds in March 2023 and for over 9 more months. If comprehensive fraud risk management had been in place before March 2023, controls could have been implemented to prevent the fraudulent withdrawals of $7.8 million.

PSC indicated that following the last reported fraudulent withdrawal in January 2024, it obtained new management, which initiated some corrective actions for weaknesses related to the Payment System processes. It also indicated in 2024 that PSC management had initiated steps to address Payment Management Services' workforce planning issues, including the high vacancy and staff turnover rates.

PSC's actions to improve fraud risk controls are a step in the right direction; however, the mitigating controls PSC put in place after the fraudulent activity were not the result of a comprehensive fraud risk management process. PSC generally has taken a reactive approach to address the fraud and loss instead of a proactive approach to implement strategies for addressing fraud risks. To more effectively protect the Payment System against sophisticated persistent threats, PSC's oversight, risk management, and mitigating controls protecting the Payment System need further strengthening based on a proactive approach to risk management and fraud prevention.

RECOMMENDATIONS

We recommend that the Program Support Center:

- implement a control environment that includes fraud mitigation, in accordance with GAO's *A Framework for Managing Fraud Risks in Federal Programs*;
- develop standard operating procedures that:
    - specify how risk and vulnerabilities to the Payment System will be regularly assessed and tested,
    - include Payment System escalation and information dissemination protocols that should be followed when a fraud incident is identified, and
    - specify verification processes for all bank accounts;
- implement automated verification processes for bank account information changes;
- finalize the bank account verification process with the Department of the Treasury for U.S.-based bank accounts;

- conduct information system level risk assessments that include integration of fraud risk in accordance with NIST guidance for all PSC financial management systems; and

- effectively implement controls for:

    - conducting required IT system vulnerability scans, reviews, and approvals; and

    - performing timely mitigation of Payment System weaknesses.

PROGRAM SUPPORT CENTER COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, PSC concurred with all of our recommendations and described actions it has taken or plans to take to address our findings and recommendations.

Regarding our first, fifth, and sixth recommendations, PSC stated that it will require contract support to: (1) implement a control environment that includes fraud mitigation; (2) integrate an assessment of fraud risk into all system-level risk assessments for PSC financial management systems; and (3) implement controls for conducting required IT system vulnerability scans, reviews, and approvals and performing timely mitigation of Payment System weaknesses. Regarding our second recommendation, PSC stated that it will develop standard operating procedures for the Payment System regarding routine assessment and testing of risk and vulnerabilities, fraud incident escalation and information dissemination, and bank account verification. Finally, regarding our third and fourth recommendations, PSC stated that it is working with the Department of Treasury on best approaches for automated verification of bank account information changes and for finalizing the bank account verification process for U.S.-based bank accounts.

PSC provided us with additional supporting documentation after the draft report was issued, and we updated the final report accordingly. PSC's comments, excluding technical comments, are included as Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

Our audit covered Payment System controls in place from March 1, 2023, through March 31, 2024, as well as the Payment System account payment details for the fraudulent transactions, which occurred between those dates.

We assessed PSC's implementation of certain cybersecurity controls prescribed for the Payment System in the following information system control areas: risk assessment; awareness and training; access; configuration management; system and information integrity; assessment, authorization, and monitoring; separation of duties; and audit event logging.

We interviewed individuals with knowledge of and responsibilities associated with the Payment System and the fraudulent activity, including PSC personnel, grant officers, and HHS Office of the Chief Information Officer personnel.

We did not assess PSC's overall internal controls. Rather, we limited our review of internal controls to those applicable to our audit objective. Specifically, we assessed the policies, procedures, and internal practices applicable to the PSC grant payment process and the protection of the Payment System.

We conducted our audit from April 2024 through December 2024 both virtually and in person at the PSC office in Rockville, Maryland.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal laws and OMB and Payment System policies, standards, procedures, and guidance related to the grant payment process, cybersecurity controls, and the protection of the Payment System;

- interviewed PSC leadership, Payment Management Services officials, contractors, host providers, and National Institutes of Health and Health Resources and Services Administration grant officers to gain an understanding of current PSC governance, grant payment processes, controls, management support activities, and Payment System cybersecurity controls and control activities;

- reviewed the information system level risk assessments for the seven financial management systems of the PSC Financial Management Portfolio: (1) the Accounting for Pay System; (2) the Debt Management and Collection System; (3) Electronic Workflow; (4) the Indirect Cost Allocation System; (5) the Revenue, Invoicing, and Cost Estimation System; (6) the Managing & Accounting Credit Card System; and (7) the Payment Management System;

- obtained and analyzed system security plans, vulnerability remediation, configuration and change management, system assessments and authorizations, and POA&Ms;

- obtained and analyzed evidence to support testing of security controls, the change management process, audit event logging, system access monitoring, and separation of duties;

- selected a nonstatistical sample of 31 PSC personnel who were required to complete Cybersecurity Awareness training, Rules of Behavior acknowledgement, and certain role-based trainings, and reviewed documentation showing completion of training;

- reviewed Payment System authority-to-operate documentation;

- verified the implementation of system security plan controls; and

- discussed the results of our audit with PSC officials.

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 the findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS

Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. section 3512, Executive agency accounting and other financial management reports and plans

This section states that the head of each executive agency establishes internal accounting and administrative controls that reasonably ensure that obligations and costs comply with applicable law; all assets are safeguarded against waste, loss, unauthorized use, and misappropriation; and revenues and expenditures are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and accountability of the assets may be maintained.

Federal Information Security Modernization Act of 2014 (FISMA), P.L. No. 113-283, section 3553

FISMA directs agencies to comply with the policies, principles, standards, and guidelines on information security promulgated under section 11331 of Title 40,[12] and to coordinate the development of their information system policies and procedures in accordance with standards and guidelines submitted by NIST under section 20 of NIST (15 U.S.C. § 278g-3). As stated in 15 U.S.C. section 278g-3(d), NIST must:

> (1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 11331 of title 40; (2) provide assistance to agencies regarding—(A) compliance with the standards and guidelines developed under subsection (a) of this section; (B) detecting and handling information security incidents; and (C) information security policies, procedures, and practices.

OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

This circular states that management in Federal agencies is responsible for implementing management practices that identify, assess, respond, and report on risks. These risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats, and identify previously unknown opportunities to improve efficiency and effectiveness of government operations. Management is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance. Management must also assess and report on the internal controls' effectiveness at least annually.

[12] 40 U.S.C. § 11331 requires that Federal information systems meet the minimum information security requirements described under section 20 of NIST (15 U.S.C. § 278g-3).

Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*

This directive establishes a mandatory, Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees) to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.

M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

This OMB memo states that to ensure secure and efficient operations, agencies of the Federal Government must be able to identify, credential, monitor, and manage all who access Federal resources, including information, information systems, facilities, and secured areas. Further, it states that agencies must implement NIST SP 800-63-3 to set the foundation for identity management.

***Standards for Internal Control in the Federal Government* (GAO-14-704G)**

The Green Book provides managers with criteria for designing, implementing, and operating an effective internal control system. The Green Book defines the standards through components and principles and explains why they are integral to an entity's internal control system.

Principle 1 states that the oversight body and management should demonstrate a commitment to integrity and ethical values through their directives, attitudes, and behavior.

Principle 7 states that management should identify, analyze, and respond to risks related to achieving the defined objectives.

Principle 8 states that management should consider the potential for fraud when identifying, analyzing, and responding to risks. Attributes to be considered are the types of fraud that can occur within the entity (including theft), fraud risk factors, and response to these risks.

Principle 10 states that management should design effective control activities to achieve objectives and respond to risks. These may be entity-level control activities, transaction control activities, or both depending on the level of precision needed.

Principle 12 states that management should implement control activities through policies. Each unit, with guidance from management, (1) determines the policies necessary and (2) documents policies in the appropriate level of detail to allow management to effectively monitor the control activity. Personnel may further define policies through day-to-day procedures, such as choosing when a control activity occurs and any follow-up corrective actions to be performed if deficiencies are identified.

Principles 13 through 15 state that management should design a process to identify the information needed to achieve the entity's objectives and address related risks. This

information, once processed into quality information, should be communicated both externally and internally (down, across, up, and around reporting lines to all levels).

Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Binding Operational Directive 19-02: *Vulnerability Remediation Requirements for Internet-Accessible Systems*

Section 3553(b)(2) of Title 44, U.S. Code, authorizes the DHS Secretary to develop and oversee the implementation of binding operational directives. Federal agencies are required to comply with DHS-developed directives. Operational Directive 19-02 states that, to ensure effective and timely remediation of critical and high-level vulnerabilities identified through Cyber Hygiene scanning, Federal agencies must: (1) ensure access and verify scope and (2) review and remediate critical and high-level vulnerabilities. The Directive further states that critical vulnerabilities must be remediated within 15 calendar days of initial detection and high-level vulnerabilities must be remediated within 30 calendar days of initial detection.

NIST SP 800-39, *Managing Information Security Risk*

NIST SP 800-39 provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of Federal information systems. This publication provides a structured, flexible approach for managing risk that is intentionally broad-based. Section 2.1, Components of Risk Management, describes the four risk management components as how organizations frame, assess, respond to, and monitor risk.

NIST SP 800-30, *Guide for Conducting Risk Assessments*

NIST SP 800-30 provides specific guidance for assessing risks in Federal information systems and organizations. Steps include preparing for, conducting, maintaining, and communicating the results of the assessment. The tasks include:

(1) Identify the information the assessment is intended to produce and the decisions the assessment is intended to support.

(2) Identify the scope of the risk assessment in terms of organizational applicability, time frame, and architectural/technology considerations.

(3) Identify the assumptions and constraints under which the risk assessment is conducted.

(4) Identify threat sources.

(5) Identify threat events that could be produced by those sources.

(6) Identify vulnerabilities in the organization that could be exploited through specific threat events and the predisposing conditions that could affect successful exploitation.

(7) Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the events would be successful.

(8) Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities through specific threat events.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*

NIST SP 800-53 provides a catalog of controls for systems and organizations to manage cybersecurity and privacy risk.

Event Logging (AU-2) states that organizations are required to identify the types of observable occurrences that the system is capable of logging in support of the audit function, and to specify the event types for logging and the frequency of logging for each type.

Information Exchange (CA-3) explains requirements for information exchanges between two or more systems. Organizations should approve and manage the exchange of information between their system and other systems using interconnection security agreements; information exchange security agreements; memoranda of understanding (MOUs); or service-level, user, or nondisclosure agreements. This section also specifies documentation, review, and update requirements for those agreements.

Penetration Testing (CA-8) states that organizations must conduct penetration testing within the organization-defined frequency on the organization-defined systems or system components.

Least Functionality (CM-7) states that organizations must configure the system to provide only organization-defined mission-essential capabilities and must prohibit or restrict the use of certain functions, ports, protocols, software, and services. Periodic reviews are completed to identify unnecessary or nonsecure functions, ports, protocols, software, and services, and disable or remove them from the system.

System Component Inventory (CM-8) states that organizations should develop and document an accurate and total inventory of system components that does not duplicate accounting of components, achieves the level of granularity needed for tracking and reporting, and includes the information the organization deems effective for system component accountability. Organizations should review and update the system component inventory to keep it complete and accurate.

Configuration Management Plan (CM-9) states that organizations should develop, document, and implement a configuration management plan for the system that addresses configuration management roles, responsibilities, processes, and procedures; establishes a process for identifying configuration items throughout the system development life cycle and for managing

the items' configuration; is reviewed and approved by organization-defined personnel or roles; and is protected from unauthorized disclosure and modification.

Vulnerability Monitoring and Scanning (RA-5) states that organizations should monitor and scan for vulnerabilities in the system and hosted applications. Further, Privileged Access (RA-5(5)) states that, in certain situations, the vulnerability scanning may be more intrusive, or the system component being scanned may contain classified or controlled unclassified information, such as personally identifiable information. Authorizing only privileged access to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Flaw Remediation (SI-2) states that the need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated personnel with information security and privacy responsibilities.

DEPARTMENT OF HEALTH AND HUMAN SERVICES POLICIES

HHS Policy for Information Security and Privacy Protection (IS2P)

Section 6.1, Baseline Security and Privacy Requirements, states that Operating Divisions must comply with the security and privacy controls in NIST SP 800-53, Revision 5, as amended.

Section 7.22, Authorizing Official (AO) or AO Designated Representative (AODR), states that the AO or AODR is a senior official with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by a system; or using a system, service, or application from an external provider. The AO or AODR is the only HHS official who can accept the security and privacy risk to the operations, assets, and individuals.

HHS Standard for Plan of Action and Milestones

Section 3.1.1, Remediation/Mitigation Timelines, states that all findings or weaknesses must be remediated or mitigated within the following timeframes:

- Critical-level weaknesses within 15 days;
- High-level weaknesses within 30 days;
- Moderate-level weaknesses within 90 days;
- Low-level weaknesses within 365 days.

Section 3.1.9, Accepting Risks and Documenting Policy Exceptions, states that long-term policy deviations, those lasting longer than 6 months, must be documented in a form reviewed by all

stakeholders and be signed by the system owner or designated representative and approved by the AO or AODR.

HHS Office of the Secretary - Payment Management System System Security Plan (SSP)

Section 15 of the SSP provides specific minimum security controls, to include:

- Plan of Action and Milestones requires any vulnerability discovered during the scanning of the system to be addressed within allotted time for severity of the findings.

- Penetration Testing requires the performance of biannual penetration testing.

- Privileged Access requires credentialed vulnerability scanning within the environment.

- Information Exchange requires that the Payment System has an MOU/interconnection security agreement with all interconnections for the Payment System, to be reviewed yearly.

- Periodic Review specifies that only authorized and required functions, ports, and protocols are in use and requires an annual review as part of the annual Payment System security assessment.

- Verification of Controls states that as the system is changed, any applicable or impacted controls are reassessed and updated if necessary. These system changes always require system-owner approval and must go through the Change Control Board.

- Event Logging requires the identification of all auditable events.

APPENDIX C: PROGRAM SUPPORT CENTER COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Program Support Center

Rockville, MD 20857

TO: Megan Tinker
Chief of Staff, Office of Inspector General

FROM: Melissa Bruce
Director, Program Support Center

MELISSA J. BRUCE -S

Digitally signed by MELISSA J. BRUCE -S
Date: 2025.04.11 19:34:25 -04'00'

SUBJECT: OIG Draft Report: *HHS's Grant Payment System Lacked Effective Internal Controls To Prevent $7.8 Million in Fraud, and HHS Has Begun Taking Corrective Actions To Reduce Fraud Risk,* A-18-24-03700

We would like to express our appreciation for the time and expertise dedicated to conducting the recent audit of the Department of Health and Human Services (HHS), Program Support Center's (PSC) Payment Management System (PMS). We have thoroughly reviewed the audit findings and recommendations, which have been valuable in identifying critical areas for improvement.

The audit revealed that "bad actors" successfully gained access to the PMS platform, resulting in the diversion of grant funds. These findings are of significant concern to us, as they highlight the urgent need to reevaluate and enhance the security and integrity of our disbursement processes within the PMS.

In response to these findings, we have taken immediate and decisive actions to address the vulnerabilities identified during the audit. We recognize the paramount importance of maintaining robust security protocols to safeguard federal funds, data, and privacy of our users. To this end, we are committed to implementing comprehensive measures to reinforce the resilience of our system against such incidents in the future.

The PSC has responded to this fraudulent activity with prompt and ongoing measures. The steps taken by PSC in addressing this issue include:

1. In January 2024, PSC leadership began meeting with grant recipients affected by the fraudulent activity after working with the Office of the Secretary, Assistant Secretary for Financial Resources and appropriators to develop a plan for restoring grant recipients' funds. PMS staff and the awarding agency took several actions to ensure the grant recipients were reimbursed for the fraudulent activity that occurred on their accounts, a process that was ultimately completed in late 2024.

2. PSC leadership reported the unauthorized access to the Computer Security Incident Response Center (CSIRC) on January 5, 2024, upon becoming aware of the incident. CSIRC subsequently reported the issue to the Cybersecurity and

Infrastructure Security Agency, which determined that it was a fraud case rather than a cyber incident.

3. On January 17, 2024, the PSC Director officially designated the PSC Chief Technology Officer (CTO) as the System Owner of PMS. This decision established a clear separation of duties between the business owner and the system owner, eliminating any previously existing ambiguities.

4. PSC began exploring methods to validate the bank account information of grant recipients. The team initially met with the Department of the Treasury on February 5, 2024, followed by discussions with the Do Not Pay team on February 23, 2024, and the Account Validation Service / Entity Validation Service (AVS/EVS) team on February 28, 2024. Afterward, bi-weekly meetings with the AVS/EVS and PMS teams were scheduled.

5. The PSC CTO and the Senior Advisor for Personnel Vetting and Identity Management immediately reviewed PMS's Identity Assurance Level[1] (IAL) and Authenticator Assurance Level (AAL) and identified two key compliance issues: grant recipients were not undergoing identity proofing, and non-HHS awarding agencies were not using Personal Identity Verification (PIV) / Common Access Card (CAC) cards for login. As a result, PMS was not compliant with NIST 800-63 and did not meet the PMS e-Authorization assessment standards of IAL3 and AAL3; the number three indicates a level three tier.

   To address this, PSC took swift action and initiated the implementation of "*ID.me*" and PSC's External User Management System in collaboration with PMS. This solution enabled grant recipients to achieve IAL2/AAL2, the highest assurance level available to the general public, while allowing non-HHS awarding agencies to use their PIV/CAC to achieve IAL3/AAL3. The implementation was completed over the weekend of February 10, 2024.

   The first communication to PMS users regarding this implementation was sent on February 9, 2024, which also acknowledged that PSC had encountered fraudulent activity. A follow-up email was issued on March 6, 2024.

6. After the implementation of *ID.me*, the perpetrator(s) adapted their approach and began targeting higher education grant recipients. They gained access to university accounts through social engineering tactics, exploiting university help desks. In response, a security alert was issued on March 14, 2024, warning users of this tactic.

   HHS, including PSC, CSIRC, and an Office of Inspector General (OIG) Special Investigator, held multiple sessions with University Chief Information Officers and Chief Information Security Officers to discuss the perpetrators' Tactics, Techniques, and Procedures (TTPs). University officials shared their experiences, provided insights into how the attacks occurred, and supplied the OIG Special

[1] NIST SP 800-63 Digital Identity Guidelines

Investigator with evidence for the ongoing criminal case.

For example, and to name a few, HHS engaged with the following institutions:

- University of Pittsburgh on March 7, 2024
- University of Colorado on March 8, 2024
- University of Louisville on March 11, 2024
- University of South Florida on March 18, 2024, which led to a broader discussion with the National Science Foundation grant system on March 19, 2024.

7. PSC also engaged with non-HHS awarding agencies to clarify the new *ID.me* requirement, as their grant recipient community was resisting its implementation. Meetings were held with the Department of State on March 4, 2024, and the Department of Labor on March 12, 2024.

8. PSC, in collaboration with the Office of the Chief Information Officer, participated in Hill briefings coordinated and led by the Assistant Secretary for Legislation (ASL). These briefings included meetings with staffers from the Senate Health, Education, Labor and Pensions Minority on March 14, 2024, and the House Committee on Oversight and Accountability Minority on March 15, 2024. For final documentation, refer to the ASL.

   The report does not acknowledge CSIRC's efforts to establish a connection to the PMS database to analyze accounts and transactions, which was critical in identifying the fraudsters' TTPs. For instance, CSIRC identified 98 accounts that required deactivation. OIG interviews with CSIRC could provide further details on these efforts.

9. From the implementation of *ID.me* through May 2024, PSC monitored the number of users who completed identity proofing to demonstrate progress to HHS leadership in achieving IAL2 for grant recipients and IAL3 for awarding agencies.

During our preliminary review of the draft OIG report, we observed an area that would benefit from additional clarification. PSC had not previously provided the OIG with the full set of supporting documentation. With the complete information in hand, the areas were refined to ensure clarity and accuracy.

Regarding the OIG recommendations that were provided as part of the audit, PSC fully concurs with all proposed recommendations. We are in the process of integrating these recommendations into our operational framework to further strengthen the PMS and ensure continued compliance with the highest standards of security and operational excellence.

The following are the OIG Recommendations included in this draft report.

1. Implement a control environment that includes fraud mitigation, in accordance with GAO's A Framework for Managing Fraud Risks in Federal Programs.

CONCUR – We will require contract support to complete this recommendation. Due to the current posture of the federal government, PSC is unsure when contract support would be available.

2. Develop standard operating procedures (SOP) that:
    a. specify how risk and vulnerabilities to the Payment System will be regularly assessed and tested,
    b. include Payment System escalation and information dissemination protocols that should be followed when a fraud incident is identified, and
    c. specify verification processes for all bank accounts.

    CONCUR – PSC will develop an SOP that covers all the areas identified in the recommendation above.

3. Implement automated verification processes for bank account information changes.

    CONCUR – PSC is working with the Department of the Treasury for best approaches.

4. Finalize the bank account verification process with the Department of the Treasury for U.S. based bank accounts.

    CONCUR – PSC is working with the Department of the Treasury for best approaches.

5. Conduct information system level risk assessments that include integration of fraud risk in accordance with NIST guidance for all PSC financial management systems; and

    CONCUR – We will require contract support to complete this recommendation. Due to the current posture of the federal government, PSC is unsure when contract support would be available.

6. Effectively implement controls for:
    a. conducting required IT system vulnerability scans, reviews, and approvals; and
    b. performing timely mitigation of Payment System weaknesses.

    CONCUR – We will require contract support to complete these recommendations. Due to the current posture of the federal government, PSC is unsure when contract support would be available.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov