Payment Integrity (Unaudited)

Background

The Payment Integrity Act of 2019 provides guidance on monitoring and reporting improper payments. Improper payments are payments made by the Government to the wrong person, in the wrong amount (either an underpayment or overpayment), for the wrong reason, or where documentation is not sufficient enough to discern whether a payment was proper.

The act reorganizes and revises several existing improper payments statutes, which establish requirements for Federal agencies to cut down on improper payments made by the Federal Government. In addition, the updated guidance also includes the following:

1. The Office of Management and Budget (OMB) may establish one or more pilot programs to test potential accountability mechanisms for compliance with requirements regarding improper payments and the elimination of improper payments.
2. The bill requires the OMB to update its plan for improving the death data maintained by the Social Security Administration and improving Federal agency use of death data.
3. Additionally, the bill establishes an interagency working group on payment integrity.

OMB Circular A-136 requires agencies to report information on payment integrity. For more detailed information on GSA's improper payments in this and previous fiscal years, visit paymentaccuracy.gov. This site includes frequently asked questions relating to improper payments, annual improper payment data sets, and program scorecards.

The U. S. General Services Administration (GSA) tested three existing programs to determine if they were at high risk for improper payments: Employee Payments, Purchase Cards, and Travel. The testing results confirmed these programs are not at high risk for improper payments.

Additionally, OMB establishes reporting requirements for programs classified as high risk or high priority for improper payment reporting. None of GSA's programs are classified as high risk or high priority for improper payment reporting.

In fiscal year (FY) 2020, GSA complied with Improper Payments Elimination and Recovery Improvement Act reporting requirements.

Payment Recapture Audit Program

The Recovery Audit Act requires agencies that award more than $500 million annually in contracts establish programs to recover overpayments to contractors. The purpose of the payment recapture audit is to identify and possibly recover overpayments. Payment recapture audits are conducted only when it is determined to be cost effective. For FY 2020, GSA had one program, Rental of Space, where a payment recapture audit was required. The Engagement Management Report for the recapture audit did not include any recommendations for corrective action.

GSA reviews the Rental of Space program annually to detect and recover overpayments or other errors, and identifies opportunities for process improvement. This review includes an analysis of lease contracts, lease amendments, and lease digest actions, as well as the development of a detailed monthly rental schedule from the beginning of a lease to its most recent payment. The results are compared to actual payments by month, to determine if discrepancies exist. Discrepancies are quantified and identified as to nature and origin.

Rent overpayments, rent credits, and real estate tax credits are common sources of overpayments. Root causes for rent-related overpayments include calculation errors, administrative errors, system errors, failure to take the proper rent credits, failure to charge rent on time or at all, and failure to timely terminate the lease. In addition, overpayments for real estate tax credits are caused by failure of the lessor to comply with the lease contract and submit tax bills or refunds, the complexity in determining the base year tax amount, and improperly determining which line items of the tax bill GSA is required to pay.

To address rent-related overpayments, GSA has taken corrective action by providing Lease Payment Audit refresher training. In addition to training, GSA implemented a change from regional to zonal administration of lease payments for taxes and other rent adjustments. Changes include proactive review of each lease annually for compliance with tax clauses and documentation, and systemic corrective action through information technology (IT) enhancements to provide national consistency and improve accuracy and timeliness.

GSA's payment recapture audit identifies claims related to the Rental of Space program. GSA establishes claims in accordance with the Debt Collection Improvement Act of 1996.

Fraud Reduction Report

In addition to being costly to taxpayers, fraud poses a serious risk to the execution of Federal programs and the ability of those programs to serve the public. To address the ever-increasing risk of fraud, Congress passed the Fraud Reduction and Data Analytics Act of 2015 (FRDAA). This act requires:

- The implementation of control activities designed to prevent, detect, and respond to fraud at GSA.
- Annual reporting on GSA's progress in implementing financial and administrative controls to identify and assess fraud risks.
- The establishment of a Government-wide fraud working group.

Guidance, implementation instructions, and the internal control framework for FRDAA are provided in:

- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016 and

GAO-14-704G, Standards for Internal Control in the Federal Government, September 2014, commonly known as the Green Book.

Fraud Reduction Activities at GSA

As required, OMB established the Fraud Working Group, which aims to improve the sharing and development of data analytics and financial and administrative controls. As part of this group, GSA and other Federal agencies contribute best practices and techniques for detecting, preventing, and responding to fraud.

In implementing these best practices and techniques, GSA leverages Government-wide tools to strengthen controls that reduce the risk of fraud against the Federal Government. For example, Do Not Pay (DNP) is an initiative mandated by the Improper Payments Elimination and Recovery Improvement Act of 2012. In order to eliminate erroneous payments, GSA screens potential vendors before awarding a contract or making a payment. Further, GSA uses the DNP database in the acquisition process where potential vendors are evaluated and cross-checked with GSA's System for Award Management (SAM) and the Internal Revenue Service's Taxpayer Identification Number Match Program.

GSA works closely with the Office of the Inspector General (OIG) to implement recommendations identified during audits and investigations. The OIG analyzes potentially fraudulent or otherwise criminal activities. It conducts nationwide criminal, civil, and administrative investigations of illegal or improper activities involving GSA programs, operations, and personnel. GSA reviews OIG reports and Semiannual Reports to Congress to help identify areas where controls could be improved.

GSA employees are privy to an abundance of information and processes for reporting fraud, and are made aware of what constitutes potentially fraudulent activity and how to report it. GSA requires its employees to complete annual training courses that cover ethics, insider threat and awareness, cybersecurity and privacy, the No Fear Act, accountability for personal property, and internal controls. This training includes modules that describe what constitutes fraudulent activity, what types of behavior are considered acceptable and unacceptable, and how and when potentially fraudulent activity should be reported. Training is updated annually to incorporate the latest fraud risk schemes. Additional information is also available to employees on the GSA employee portal, InSite.

On an annual basis, GSA assesses compliance with the Government Accountability Office's (GAO) 5 components and 17 principles of internal control. This assessment specifically includes requirements from the Green Book principle 8 - Assess Fraud Risk. The results are analyzed to identify internal control issues or concerns. GSA's senior assessment team, the Management Control and Oversight Council (MCOC), reviews the results, including fraud risk, to ensure findings are appropriately addressed in the Administrator's Annual Statement of Assurance. The MCOC provides a structure for GSA's senior management to convene and provide the leadership and oversight necessary to implement and maintain the agency's internal control program.

GSA addressed fraud at the program level through annual internal program reviews, which include a risk assessment. GSA has a total of 360 internal control reviews, which it evaluates over a 5-year cycle. In FY 2020, the reviews did not identify any material weakness or significant deficiencies.

GSA COVID-19 Pandemic Response

In response to the COVID-19 pandemic, on March 27, 2020, President Trump signed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (P. L.116-136) into law. GSA published the CARES Act Financial Internal Control Plan, describing how GSA planned to mitigate fraud risks. As a part of this effort, GSA outlined the use of funds, identified potential risk for fraud, established controls for spending, and highlighted reporting requirements.

GSA established the Executive Reporting and Management Oversight team to provide GSA leadership with executive-level reporting on COVID-19 activities. This group provides routine communications to senior leadership and tracks COVID-19 program implementation, strategic cohesiveness of response efforts, and cross-program coordination. In addition, policy updates are continually monitored and shared with GSA leadership for dissemination to applicable organizations.

Funds used to perform COVID-19 response activities are tracked using specific CARES Act fund and project codes. Spending is monitored regularly to validate funds are used for their intended purpose. Each month, GSA prepares and submits an executive summary to leadership describing COVID-19 spending and compliance with authoritative guidance.

Combating fraud is a collaborative effort for GSA. GSA Services, Staff Offices and Independent Offices play a vital role in identifying and preventing fraud. Included in the following are strategic efforts by each.

GSA Services

Public Buildings Service

The Public Buildings Service (PBS) works in close coordination with its business partners — including the OIG, the Office of Government-wide Policy (OGP), the Office of the Chief Financial Officer (OCFO), and the GAO — to strengthen controls and reduce the risk of fraud. PBS collaborates with these entities to implement recommendations and corrective actions that mitigate risks associated with fraud across its business processes. PBS has enhanced and automated its processes to improve transparency and reduce fraudulent activity. PBS complies with internal policies for requesting, tracking, and approving transactions.

Additional acquisition fraud detection activities include:

- Prior to lease award, PBS verifies offeror eligibility for participation in Federal contracts using the Exclusions Extract available in the SAM database, which requires contractor registration. By verifying potential contractors are not debarred or suspended, GSA is able to more effectively limit its potential for fraudulent activity in its leasing program.

- PBS tracks its payments for lease projects using the GSA Real Estate Exchange and Real Estate Across the U.S. systems to identify project or payment anomalies that potentially reflect fraudulent activity.
- PBS worked with OCFO to implement a receiving report module in the acquisition system to enable receipt and payment of services electronically, thereby eliminating duplicative entries. The interfacing accounting system helps to identify project or payment anomalies that potentially reflect fraudulent activity.

Federal Acquisition Service

FAS works hand-in-hand with OCFO to mitigate risks associated with fraudulent financial reporting and the misuse of assets. Segregation of duties is incorporated in its financial, travel, and procurement systems. Specifically, transactions including purchase requests, travel authorizations, and credit card purchases are approved by a fund manager and certified by an independent OCFO official, validating internal control compliance.

Additional program-specific fraud detection activities include:

- FAS' National Customer Service Center uses best practices, including customer identity verification procedures, for identifying potential fraud when customers place orders with GSA.
- GSA Fleet has a loss-prevention team that uses routine reports to monitor GSA fleet cards for fraud, waste, and abuse.
- The Acquisition Center Multiple Award Schedule program proactively completes contractor assessments within the program to review compliance with contract terms and conditions. This review includes correctness of reporting, overcharges, scope, Trade Agreement Act, and other contract requirements. The findings have resulted in recovered funds of over $6.8 million in FY 2020. Issues of compliance are tracked and contracting officers and contracting specialists are provided a status for assigned contracts.
- SAM is the centralized service that supports Federal acquisition and financial assistance awards managed by the GSA Integrated Award Environment (IAE) program management office. When upgrading SAM, GSA ensured fraud vulnerabilities were implemented using a third party to evaluate and test the program.
- SAM supported 296 active fraud investigations in FY 2020, providing detailed system records and audit data to the GSA OIG and other agencies' inspectors general. The data and subject matter expertise provided by the IAE program was critical in multiple successful inter-agency prosecution efforts, and demonstrates GSA's ongoing commitment to fighting procurement and supply chain fraud.
- FAS educated users and increased awareness of phishing and deceptive, unsolicited email practices employed by companies not affiliated with the Government. IAE updated its help content

and shared instructions for users to identify and report potential suspicious activity by leveraging resources in the U.S. Computer Emergency Response Team, the Federal Bureau of Investigation, and the Federal Trade Commission.

GSA Staff Offices

Office of Administrative Services

The Office of Travel and Charge Card Services established a centrally billed account and contracted a vendor to monitor travel card payments and transportation expenses, respectively. The vendor performs an automated reconciliation of travel transportation billings and provides GSA with a list of reconciled charges. There are no delinquencies on this account since it is paid on a bi-weekly basis.

For individually billed accounts, GSA automated the process for providing each cardholder's supervisor with a monthly delinquency report, resulting in improved timeliness, increased transparency, and deterred fraudulent activity. Supervisors counsel and discipline employees, as necessary, in consultation with the Office of Human Resources Management (OHRM).

To mitigate the risk associated with employees who separate from GSA and fail to properly return or destroy their charge cards, GSA uses a daily employee separation list to verify active card holders. The accounts of employees who have separated are immediately canceled with U.S. Bank. As an additional control, a monthly separation list from OHRM is used to verify the accounts for separated employees that may have been missing from the daily list and are closed with U.S. Bank. GSA reconciles the list of active U.S Bank charge card participants to human resource files on a periodic basis, at least once a year.

GSA uses state of the art credit card monitoring practices to ensure the legitimate use of its purchase and travel cards. These include:

- Leveraging U.S. Bank's payment analytic tool to flag questionable transactions and ensure transactions are not split to bypass purchase card limits. All flagged activity is further investigated and determined to be valid or recommended for disciplinary action.
- Monitoring retail blocks on questionable or high-risk Merchant Category Codes for purchases and travel, and reviews and updates the use of these codes periodically.

GSA requires all approving officials, cardholders, and agency and organization program coordinators to complete training prior to appointment and issuance of a charge card for purchase or travel, in addition to completing a refresher training every 2 years for travel cards and every 3 years for purchase cards.

Office of Government-wide Policy

The Procurement Management Review (PMR) Division ensures that adequate internal controls for procurement activities are in place and operating as designed. These reviews identify ways to strengthen controls that reduce risks. If instances of potential fraud surface, the PMR Division will contact the GSA OIG.

The Suspension & Debarment Division reviews reports of confirmed or alleged fraud in public contracting. Based on these reports, the division considers whether suspension or debarment from Federal Government contracting is required. The division can penalize contractors by means other than suspension and debarment to protect the Government from fraud and other contractor misconduct. Once a final decision is made regarding suspension or debarment, SAM is updated, alerting contracting officers. Ensuring SAM is up to date reduces the risk of contracting officers procuring services from suspended or debarred contractors.

OGP's Office of Information Integrity and Access manages the .gov top-level domain registry for Federal, State, Tribal, and local governments. OGP uses a variety of methods and techniques to prevent bad actors from obtaining a .gov domain under false pretenses. All applicants are carefully vetted and verified through multiple third-parties, per individual request. On a limited number of occasions, OGP has engaged the GSA OIG to investigate fraudulent domain registration attempts that have been detected.

OGP manages the Federal Identity, Credential, and Access Management program. In this capacity, OGP partners with the OMB and the National Institute of Standards and Technology to ensure Federal agencies have policy-compliant solutions to assert the identities of Federal and contractor employees and that agencies purchase policy-compliant physical access security systems.

Lastly, OGP manages the Federal Public Key Infrastructure (PKI) Policy Authority by setting policy governing the Federal PKI Trust Infrastructure, approving applicants for cross certification with the Federal Bridge Certification Authority, and providing oversight to the Certified PKI Shared Service Provider Program.

Office of the Chief Information Officer

The Office of GSA Information Technology (GSA IT) seeks to reduce and prevent fraud through a progressive, integrated approach, capitalizing on cutting-edge technical solutions. For example, in May of this year, GSA IT introduced program-level changes in the SAM/IAE environment to correct and prevent instances of suspended and debarred contractors from obtaining awarded contracts. As a part of this effort, the DNP database is updated daily to tag suspended or debarred vendors and reduce the likelihood that a contract is awarded to an unauthorized provider.

For FAS business systems GSA Advantage!® and GSA eBuy!, GSA IT integrated a third-party identity management solution to provide multi-factor authentication (MFA). GSA IT's ASSIST team implemented MFA for all external vendors and Federal clients. MFA was also implemented for the Office of Personal Property Management websites GSAXcess, GSAAuctions and MySales by August 2020. Since MFA requires a user ID and password, as well as a one-time password, it reduces the risk of unauthorized access and provides extra security for customers, including Federal agencies, State and local governments, non-profit organizations, and the general public.

GSA IT tracks and retains user traces so historical data is available for OIG investigations in an effort to reduce fraud in the Computers for Learning program.

For the Fleet program, the loss-prevention team identified several functions where fraudulent activities are both possible and tempting. Specifically, analysts look for anomalies in fuel usage by tracking vehicle fuel consumption rates (miles per gallon/mpg) and the amount of fuel dispensed. By developing multiple dashboards, analysts can drill down to review a specific transaction via the vehicle identification number and identify all relevant vehicles that have fuel consumption anomalies. The Overtank and Miles per Gallon dashboards are two that are used to detect fraud. Following an investigation, the analysts forward suspected fraud to the GSA OIG or mark it as false positive. In addition, the Fleet loss-prevention team has deployed ad hoc capabilities so that a robust data exploration is available to the analysts.

GSA IT's infrastructure support teams provide a weekly report of web applications' user login and logout activities to the GSA IT security and financial management teams. This report enables anomaly detection and can indicate patterns that may be indicative of fraudulent activity.

Additional steps have been taken this year to prevent fraudulent software use by reconciling user software licenses and encouraging self reporting for active licenses. As a part of the annual user recertification process, licensed users are asked to report on the status of active software licenses.

GSA IT continues to focus expertise and resources on preventing fraud through tracking and minimizing the use of social security numbers requiring all employees and contractors to complete annual IT security and privacy training, and using detection and prevention tools on outbound email to flag sensitive information such as personally identifiable information.

Office of the Chief Financial Officer

OCFO is committed to developing and maintaining the financial management knowledge and skills of its staff. In this vein, OCFO offers continuing education opportunities focused on financial management. Additionally, offices within OCFO participate in trainings tailored to specific job tasks. For example, in an effort to address prior audit findings, applicable offices within OCFO participated in Antideficiency Act training. Maintaining training beyond fraud reinforces the importance of proactively mitigating risks through good stewardship of funds and sound financial management, creating an atmosphere of professional accountability.

Additional oversight occurs when the OCFO Payroll Services Branch and the Payroll Accounting and Reporting (PAR) system are audited annually. These audits include service organization controls, agreed-upon procedures on behalf of GSA, and multiple client-agency financial statement audits. The testing performed during these audits includes reviewing:

- The payroll system access, calculations, and processing controls;
- The entirety of the OCFO Payroll Services Branch processes and controls; and
- The accuracy of the payroll reporting to the financial systems.

The OCFO payroll operations team has stringent controls in place for the certification and transmission of payment files to the U.S. Department of the Treasury for the actual fund disbursements to payees via Treasury's Secure Payment System. Payroll disbursement transactions and processes, and the controls over them, are regularly reviewed by the payroll supervisors and are included in the scope for the annual audits performed. Fraud has not been detected or reported on by the payroll staff, IT support staff, related operations, or the PAR system.

OCFO payroll operations team does receive periodic OIG investigative requests for employee pay, time, and attendance data from the payroll system. This information is provided in full and in the strictest of confidence.

The primary concern of the OCFO payroll operations is ensuring that all certified time and attendance actions are processed timely and accurately for disbursement. An action certified is presumed to be accurate and authorized for processing and subsequent disbursing. The retroactive payroll system process is available when agency employees, supervisors, and HR officials identify administrative errors have been made in the originally processed transactions or time cards. In these instances, the employee, supervisor, and HR official prepare, certify, and process retroactive actions to correct or adjust the previously submitted transactions.

In addition, OCFO has made progress identifying risks and vulnerabilities to fraud with respect to payroll and beneficiary payments. The time management system integrates leave requests with the time cards and reduces risks associated with paying employees improperly. Controls reduce the risk of paying employees after separation.

GSA Independent Offices

Office of Inspector General

Integrity Awareness

The OIG presents integrity awareness briefings nationwide to educate GSA employees on their responsibilities for the prevention of fraud and abuse. This period, the OIG presented 20 briefings attended by 1,332 GSA employees, employees from other Government agencies, and Government contractors. These briefings explain the statutory mission of the OIG and the methods available for reporting suspected instances of wrongdoing. In addition, through the presentation of case studies, the briefings make GSA employees aware of actual instances of fraud at GSA and other Federal agencies and thus help to prevent their recurrence. GSA employees are the first line of defense against fraud, abuse, and mismanagement. They are a valuable source of investigative information.

Semiannual Report to Congress

The GSA OIG plays a significant role in the prevention and detection of fraud at GSA, including through OIG investigations, the Suspension and Debarment Initiative, and the OIG Hotline. An overview of each, as well as GSA's FY 2020 incidents included in the Semiannual Reports to Congress (SAR), follows.

- OIG Investigations - The Office of Investigations conducts independent and objective investigations relating to GSA programs, operations, and personnel. The office consists of special agents with full statutory law enforcement authority to make arrests, execute search warrants, serve subpoenas, and carry concealed weapons. Special agents conduct criminal, civil, or administrative investigations that often involve complex fraud schemes. Investigations can also involve theft, false statements, extortion, embezzlement, bribery, antitrust violations, credit card fraud, diversion of excess Government property, and digital crimes.

2020 SARs	October 1 - March 31	April 1 - September 30	Total
Opened Investigative Cases	70	53	123
Closed Investigative Cases	72	62	134
Subjects Referred for Criminal Prosecution	262	88	350
Helped Obtain Convictions	17	12	29
Monetary Recoveries	$2,027,085	$89,947,634	$91,974,719

Suspension and Debarment Initiative - GSA has a responsibility to ensure the people and companies it does business with are not excluded parties, which are individuals or organizations that have been declared ineligible to receive Federal contracts. The Federal Acquisition Regulation authorizes an agency to suspend or debar individuals or companies for the commission of any offense indicating a lack of business integrity or business honesty that directly affects the present responsibility of a Government contractor or subcontractor. The OIG has made it a priority to process and forward referrals to GSA, ensuring the Government does not award contracts to individuals or companies that lack business integrity or honesty.

2020 SARs	October 1 - March 31	April 1 - September 30	Total
Referrals for Consideration of Suspension or Debarment	92	32	124
Actions Issued Based on Referrals	104	73	177

- OIG Hotline - GSA maintains the OIG hotline, providing employees the opportunity to anonymously report suspected wrongdoing that could adversely impact GSA. Additionally, GSA uses signage within GSA controlled-buildings to offer further guidance to employees regarding the OIG hotline's intended purpose and direction for the submission of inquiries. Finally, the OIG also allows employees to submit online complaints. The OIG is intentional in efforts to offer employees and other concerned citizens multiple avenues to report suspected cases of intentional or unintentional fraud.

2020 SARs	October 1 - March 31	April 1 - September 30	Total
Received Hotline Contacts	650	488	1,138
Hotline Contacts Referred for Review and Appropriation Action	60	40	100
Referred to Other Federal Agencies	14	2	16
Referred to OIG Office of Audits	17	21	38
Referred to Investigative Field Offices	69	56	125