FRAUD **REDUCTION REPORT** (UNAUDITED)

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

- Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016
- 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 (TIN) Match Program.

GSA also works closely with the Office of 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 (SAR) to help identify areas where controls could be improved.

GSA employees are exposed to an abundance of information and processes for reporting fraud, and should be well aware of what constitutes potentially fraudulent activity and how to report it. GSA requires its employees to complete annual training courses that include ethics, insider threat and awareness, cybersecurity and privacy, the No Fear Act, and accountability for personal property. All have training modules that describe what constitutes fraudulent activity, what types of behavior are considered acceptable and unacceptable, and how and when potential fraudulent activity should be reported. In addition, prohibited personnel practices and whistleblower posters are prominently displayed in GSA buildings. Additional information is also available to employees on the GSA portal, InSite.

GSA revamped methods to evaluate compliance with the Government Accountability Office's (GAO) 5 components and 17 principles of internal control, including principle 8, the fraud risk principle. The revised Internal Control and Evaluation Tool was completed by 14 Heads of Services and Staff Offices. Fraud risk is discussed by the GSA senior assessment team, the Management Control and Oversight Council (MCOC), to ensure it is appropriately addressed in the Administrator's Annual Statement of Assurance.

In FY 2019, the MCOC meetings included discussions on the status of corrective actions for outstanding audit findings from the annual external financial statement audit and the annual internal control plan. At the conclusion of the fiscal year, MCOC members completed a survey to identify internal control and fraud issues not previously reported with no areas of concern identified.

GSA addressed fraud at the program level through annual internal program reviews, which included an assessment of risk. GSA has a total of 360 internal control reviews, which it evaluates over a 5-year cycle. In FY 2019, GSA performed all 64 of its planned internal control reviews.

GSA Services and Staff Offices play a vital role in identifying and preventing fraud. Prior to the Fraud Reduction Act, GSA had already implemented measures to reduce fraud and has provided an overview of the measures taken by each office below:

Office of the Chief Information Security Officer conducted a fraud and risk assessment of the SAM database (**SAM.gov**) in the third quarter of FY 2019 to identify existing web application vulnerabilities and business process flaws in the SAM application that could be exploited by an adversary to commit fraud. The assessment was primarily focused on the validation of business processes within SAM and its third-party dependencies. Penetration tests and passive (non-intrusive) testing were also conducted against in-scope assets against externally accessible third-party applications.

Office of Public Buildings Information Technology Services assisted in adding more robust requirements for contractors in the GSA Leasing Support Services (GLS) contract:

- The GLS contract was reviewed to identify options to protect GSA data. The ultimate decision was to have all GLS contractors use GSA Information Technology (IT) systems and not allow them to stand up their own systems to support. This will ensure that IT systems used to store Government data meet GSA, Federal Information Security Management Act of 2002, and National Institute of Standards and Technology requirements.
- Contractors are not permitted to use non-GSA services, systems, or email unless specific exceptions have been granted.
- The GLS Plus Virtual Preproposal Conference was held in July for prospective bidders. This conference provided additional details on the main contract requirements, the use of GSA IT systems, required background clearance process, and IT training.

Bringing the contractors in-house on GSA systems ensures greater process and implementation control.

A third-party identity management solution has been integrated into Federal Acquisition Service (FAS) business systems GSA Advantage!® and GSA eBuy!® to implement multi-factor authentication. Users of both sites are now required to provide a time-based, one-time password at the time of login, in addition to a user ID and password. Among the many features included are:

- Government purchaser validation
- User validation of all requests for quotes (RFQ) created in eBuy!®
- Application-level auditing to:
    - prevent fraudulent RFQs and fraudulent purchases,
    - provide automatic reviews of credit card usage patterns,
    - run automated scripts for new user registration validations every 2 hours, and
    - run automated scripts to detect and block search engine robots, or spiders, from accessing GSA Advantage!® data.

Office of Enterprise Infrastructure Operations' fraud reduction activities include:

- **Computers For Learning (CFL):** GSA IT has been reviewing the functions that local support does internally as well as the functions of other entities in GSA that involve IT. As customers of the FAS' personal property disposal program GSAXcess, GSA IT transfers surplus computers to educational institutions via the CFL program. To reduce the possibility of fraud, GSA IT has started revalidating the eligibility and authenticity of schools prior to each transfer, including for repeat customers. In the past, GSA only performed a validation prior to the first transfer. Validations also now include specific source checks based on enhanced guidance received from the Office of Administrative Services (OAS).

- **Identity and Access Management:** GSA IT is transitioning more and more applications to the SecureAuth single sign-on solution, which has integrated two-factor authentication for identity and access management services. In addition, GSA IT is adding various application-specific access requests in the enterprise IT service management platform ServiceNow that require documented approvals from application owners prior to granting access to the specific application.

- **Software Asset Management:** GSA IT Infrastructure Operations Division has incorporated increasingly mature software asset management capabilities and toolsets into the GSA software approval process. Improved processes and capabilities lower the risk of accidental fraud by contacting each software requester to ensure the proof of purchase and license use agreement are collected prior to authorizing installation of the requested software.

In addition to these more recent additions to GSA IT's fraud prevention efforts, there are other actions that are routinely deployed to prevent fraudulent misuse of information. Other steps taken are:

- Tracking and minimizing the use of social security numbers (SSN)
    - GSA does not include the SSN of an individual on any document sent by postal mail, except as authorized by the Administrator or as required by applicable law, regulations, or Government-wide policies (e.g., U.S. Department of the Treasury–Internal Revenue Service Form W-2, Wage and Tax Statement, which GSA must provide to each employee).
    - The only GSA-sponsored forms requesting a full SSN on a voluntary basis are GSA 3665 – Authorization to Obtain Credit Report and GSA-850 – Contractor Information Worksheet.

- Requiring annual IT security and privacy training for employees
- Using detection and prevention tools on outbound email, including:
    - CloudLock, which identifies privacy and security risks, and
    - MailGate, which quarantines outbound traffic to reduce the release of SSNs in an unencrypted format. Quarantined emails are monitored on a daily basis by GSA Privacy Office staff.

Each of these actions are annually reported on as required by the Social Security Number Fraud Prevention Act of 2017 (Pub. L. 115-59).

Office of the Chief Financial Officer

In addition to the agency-wide training that educates GSA employees on potential fraud, OCFO team members successfully completed training on the Antideficiency Act and an Overview of Financial Management.

Additional oversight occurs when the OCFO Payroll Services Branch and 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 but is not limited to 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 has stringent controls in place for the certification and transmission of payment files to U.S. Department of the Treasury for the actual fund disbursements to payees via Treasury's Secure Payment System. The 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 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 results of these OIG inquiries are never shared with the OCFO payroll operations.

The primary concern of the OCFO payroll operations is to ensure 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. A new time and attendance system was implemented in the third quarter of FY 2018, which integrated leave requests with the time cards and reduced the risk associated with paying employees improperly. Controls were also strengthened to reduce the risk of paying employees after separation.

Public Buildings Services

The Public Buildings Services (PBS) works in close coordination with its business partners — including the OIG, the Office of Government-wide Policy (OGP), 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 program-specific fraud detection activities include:

Lease Acquisition

- The Office of Leasing works with OGP to conduct Procurement Management Reviews (PMR) of leases and PBS's compliance with leasing policy and procedures. All findings from PMR audits are shared with the OIG, and OGP notifies the OIG of any suspicious or potentially fraudulent activities detected during the PMR review of real property leases.
- Prior to lease award, PBS determines that each offeror is eligible for participation in Federal contracts using the exclusions extract available in the SAM database. By verifying that its potential contractors are not debarred or suspended, GSA is able to more effectively limit its potential for fraudulent activity in its leasing program.
- Prior to lease award, PBS requires that offerors be registered in the SAM database, which supports PBS in its efforts to manage risk for potential fraudulent activity in its leasing program.
- PBS also tracks its lease projects using the GSA Real Estate Exchange and Real Estate Across the U.S. systems for lease payments that could identify project or payment anomalies that potentially reflect fraudulent activity.

Acquisition

- The OIG conducts audits on high-value, high-risk PBS contracts.
- PBS works to implement recommendations identified during audits and investigations. The OIG analyzes potentially fraudulent or otherwise criminal activities. They conduct nationwide criminal, civil, and administrative investigations of illegal or improper activities involving PBS programs, operations, and personnel.
- PBS reviews OIG reports and develops corrective action plans in coordination with applicable business lines to mitigate risks associated with findings.
- PBS worked with OCFO to implement a receiving report module in the Enterprise Acquisition System Integrated (EASi) to enable receiving and payment of services electronically, eliminating duplication of entry in EASi and the interfacing financial management system, Pegasys, helping to identify project or payment anomalies that potentially reflect fraudulent activity.

Federal Acquisition Service

FAS operations work hand-in-hand with OCFO to mitigate risks associated with fraudulent financial reporting and misuse of assets. Automated processes with restricted access, and required third-party approvals for obligating funds and approving expenditures in systems such as Pegasys, ConcurGov travel, various commercial applications, and the Information Technology Support Services/Assisted Services Shared Information System in the acquisition arena, have minimized the potential for inappropriate activities to occur. Segregation of duties is established in these systems with regard to internal financial controls to ensure transactions, including purchase requests, travel authorizations, and credit card purchases, are approved by a fund manager and certified by an independent OCFO official.

Additional program-specific fraud detection activities include:

- FAS' National Customer Service Center (NCSC) uses best practices, such as customer identity verification procedures, for identifying potential fraud when customers place orders with GSA. NCSC has coordinated internally with the OIG on numerous fraud-related investigations.
- GSA Fleet has a Loss Prevention Team that uses routine reports to monitor GSA fleet cards for fraud, waste, and abuse. The team has an agreement with GSA's OIG to perform investigations when Fleet turns the information over to the OIG.
- Acquisition Center Multiple Award Schedule (MAS) programs work in collaboration with the OIG to resolve findings in pre-award examination audit reports of the MAS vendors. These findings often involve vendors overcharging the Government or not paying the required amount of GSA's industrial operations fees. Similar findings are researched by the FAS industrial operations analysts and have resulted in potential recovered funds of nearly $180,000 during the first half of FY 2019. This information is turned over to administrative contracting officers to resolve.
- SAM is a SAM is the centralized service that supports Federal acquisition and financial assistance awards managed by the GSA Integrated Award Environment program management office. In FY 2019, GSA tested the controls implemented in FY 2018 and built upon them. GSA commissioned a comprehensive third-party fraud and risk assessment of both legacy SAM and the beta.SAM.gov modernization effort. The assessment sought to identify existing web application vulnerabilities and business process flaws. Only minor issues were identified within the SAM application itself. Several inherited risks were identified from an external interface. These were shared with the provider and addressed in a timely manner. GSA considers the use of the third-party assessment team essential to vigilant protection of data.
- SAM alone supported more than 220 active fraud investigations, providing detailed system records and audit data to the GSA OIG and other agencies' inspectors generals. The data and subject matter expertise provided by the IAE program was cited numerous times as being critical to multiple successful, inter-agency prosecution efforts and demonstrates GSA's ongoing commitment to fighting procurement and supply chain fraud.
- GSA took steps to help educate users and increase awareness of phishing and deceptive, unsolicited email practices employed by some companies not affiliated with the Government. IAE updated its help content and shared instructions for users to identify and report potential suspicious activity — including unsolicited email or other unsolicited contact, and phishing — by leveraging resources at the U.S. Computer Emergency Response Team, the Federal Bureau of Investigation, and the Federal Trade Commission.

Additionally, GSA has multiple new controls to deter fraudulent activity in the SAM. These controls include:

- Implementing multi-factor authentication to log into SAM.gov. This requires a SAM user to be double validated by a username and password and by entering a unique code sent to an electronic device associated with a user account during the login process.

- Restricting access to the expired registration data migrated into SAM from the Central Contractor Registration system in 2012, which has never been activated in SAM. This deters bad actors from using inactive registration information to impersonate a legitimate business.
- Notifying vendor and the parent entity when the vendor changes bank information in the registration. This reduces the risk of undetected financial information changes and misdirected payments. Parent approvals are also required if a child entity tries to register in SAM.

Partially masking sensitive data (i.e., displaying a TIN as *****3928 to someone logged into the system). This added to the existing control (which prevented public display of sensitive data) by not displaying full sensitive fields even to users with roles to the entity, reducing the risk of exposing data should a bad actor gain access to a registration. SAM only displays the last four characters of the Marketing Partner Identification Number, TIN, ABA routing number, and bank account number for users with approved roles.

Office of Administrative Services

GSA Travel and Purchase Card Programs

Reducing Travel Card Delinquencies

To monitor delinquencies associated with the travel card, GSA established a centrally billed account with the contracted Electronic Travel System (ETS) vendor for travel transportation expenses. The ETS 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, a monthly delinquency report is provided to each cardholder's supervisor. Approving officials (AO) counsel and discipline employees, as necessary, in consultation with the Office of Human Resources Management (OHRM). GSA initiates salary offset to collect undisputed delinquent travel charge card debt. To further reduce the potential for delinquent accounts, GSA has incorporated the split disbursement feature into ETS for payment directly to the charge card contractor.

There are no delinquencies for the purchase card program since payment to the charge card contractor is made on a daily basis.

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 and verifies the names on the list. These accounts are immediately canceled with U.S. Bank. As an additional control, a monthly separation list from OHRM is used to verify closing separated employee accounts with U.S. Bank that may have been missing from the daily list. GSA also reconciles the list of active charge card participants from U.S. Bank to human resource files on a periodic basis, at least once a year.

Additional Travel and Purchase Card Controls

GSA program offices receive a semiannual report of inactive purchase cardholders (accounts with no activity in the preceding 12 months) for review. The program offices initiate closure for accounts that are no longer needed.

GSA uses retail blocks on questionable or high-risk Merchant Category Codes (MCC) for purchases and travel. GSA reviews and updates the use of these codes periodically.

Travel card applicants complete their travel card application online in lieu of completing a paper application. The online application increases sustainability by reducing the number of paper applications processed and increases the security of an applicant's personally identifiable information.

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 and complete refresher training every 2 years for travel cards and every 3 years for purchase cards.

Charge card program improvements in FY 2019 include:

- Sending monthly questionable charges and delinquency reports to OHRM to ensure approving officials and supervisors carry out consistent application of disciplinary action, when necessary.
- Using a new commercial off-the-shelf data mining tool, Insight on Demand (IOD). This tool reduces the risk of misuse by regularly identifying questionable charges.
- Limiting cash withdrawals to 2 percent of the cardholder's travel card limit. This strategy will reduce excessive ATM withdrawals on the travel card, reduce ATM fees, and increase GSA's rebate on the use of the travel card.
- Developing and implementing a policy for the use of third-party payment providers.
- Using U.S. Bank's payment analytic tool to flag questionable transactions to ensure transactions were not split in order to bypass purchase card limits.

GSA uses the following reports to detect possible charge card misuse:

Pegasys Daily Charges Report- This report is used by cardholders to review daily transactions. Credit card vendors import transaction data into Pegasys, generating email notifications to cardholders on the availability of their daily transaction report. Cardholders can then download, review, and verify the report.

Pegasys Monthly Charge Card Transaction Report- This report is used by AOs to review their cardholders' monthly transactions. The Pegasys charge card module automatically sends an email to the AOs, including a consolidated report of all their cardholders' monthly charge card transactions. AOs can elect to receive daily emails of new charge activity as it occurs, and they can access a variety of reports on their cardholders' accounts at any time from the Pegasys reports module. All AOs are required to review and certify their monthly reports within 10 days of receipt and take action on all unauthorized and questionable charges. In addition, the OAS monitors the AOs' monthly reviews to ensure completion.

Questionable Charges Report- This report uses IOD to assess questionable transactions. On a monthly basis, OAS uses data mining techniques to identify questionable charges using attributes such as:

- Merchant description;
- MCC;
- Merchant names;
- Holiday transactions; and
- Key words.

The data is reviewed and compiled into questionable charges reports for further review.

The GSA OIG has direct access to all purchase and travel card data and performs limited data mining on purchase card transactions. In addition, the program office contacts the OIG if inappropriate use of the card is discovered. The GSA OCFO A-123 review team conducts a quarterly review of internal controls in accordance with the Improper Payments Elimination Recovery Act of 2010.

Impending Suspensions Report – OAS notifies regional coordinators to follow up with AOs who have not reviewed and certified their Pegasys monthly transactions. Upon notification, the AOs have 10 days to review and certify the Pegasys reports to prevent the suspension of their cardholders' accounts.

Transaction File – This monthly nationwide file of all purchase card transactions is provided to the GSA OIG and the Federal shared service provider for financial services for review and audit sampling.

Potential Split Transactions – These transactions are monitored daily for policy violations. In the event of a violation, OAS advises the AO and management officials to take corrective action in consultation with their servicing human resources office. OAS also reports the violation to the OIG.

Travel Card

The questionable charges reports described above are also utilized for travel cards. In addition, OAS uses data mining attributes such as:

- Merchant description;
- Cash;
- MCC;
- Merchant names;
- Returned checks; and
- Travel card transactions that are not supported by an approved travel authorization in ETS.

Additional Control to Curb Fraud

Lost and stolen card reports are run annually to identify cardholders who report their purchase card lost or stolen during the period. The report is used to monitor potential fraud and abuse of the purchase card. OAS may revoke a cardholder's purchase card and refer the cardholder to the OIG if fraud or abuse is detected.

Office of Inspector General

Fraud Prevention Strategies and Procedures

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 121 briefings attended by 1,746 GSA employees, other Government employees, 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 in 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.

OIG Semiannual Report to Congress

The GSA OIG plays a significant role in the prevention and detection of fraud at the GSA and reported the following activities during FY 2019.

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. During this reporting period, the office opened 116 investigative cases, closed 110 investigative cases, referred 159 subjects for criminal prosecution, and helped obtain 49 convictions. Civil, criminal, and other monetary recoveries resulting from OIG investigations totaled over $122 million.

Suspension and Debarment Initiative

GSA has a responsibility to ascertain whether the people or companies it does business with are eligible to participate in Federally assisted programs and procurements, and to ensure that they are not excluded parties, which are individuals or companies 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 that the Government does not award contracts to individuals or companies that lack business integrity or honesty.

During this reporting period, the OIG made 130 referrals for consideration of suspension or debarment to the GSA Office of Acquisition Policy. GSA issued 226 actions based on current and previous OIG referrals.

OIG Hotline

The OIG hotline provides an avenue for employees and other concerned citizens to report suspected wrongdoing. Hotline posters located in GSA controlled buildings encourage employees to use the hotline. The hotline also allows internet submission of complaints. During the reporting period, the OIG received 1,304 hotline contacts. Of these, 152 were referred to GSA program officials for review and appropriate action, 30 were referred to other Federal agencies, 23 were referred to the OIG Office of Audits, and 127 were referred to investigative field offices for investigation or further review.