

FRAUD REDUCTION REPORT

Agency progress on implementing the Fraud Reduction and Data Analytics Act of 2015 (Pub. L. 114-186, 31 USC 3321):

The Fraud Reduction and Data Analytics Act of 2015 requires annual reporting on the Agency's progress in implementing financial and administrative controls to identify and assess fraud risks. The Act also requires the agency to implement control activities designed to prevent, detect, and respond to fraud, including improper payments. Guidance, implementing instructions, and the internal control framework are provided in:

- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016; and
- GAO-14-704G, The Standards for Internal Control in the Federal Government, September 2014 (the Green Book)

GSA uses Federal solutions to strengthen controls that reduce the risk of fraud against the Federal Government. For example, the DNP solution is a Governmentwide initiative mandated by the Improper Payments Elimination and Recovery Improvement Act of 2012 to screen payment recipients before a contract award or payment is made in order to eliminate payment errors. GSA has incorporated this mandate into our business processes. The DNP database is also used in the acquisition process. Prior to contract award the DNP is reviewed as part of the evaluation process, as well as GSA's SAM and the Internal Revenue Service's Taxpayer Identification Number (TIN) Match Program.

GSA works closely with the OIG 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 GSA programs, operations, and personnel. GSA reviews OIG reports and the Semi-Annual Report to Congress to help identify areas where controls could be improved.

In FY 2018, the OIG identified fraudulent activity in the SAM database. GSA implemented multiple preventive measures to fix these controls including:

1. Multi-factor authentication to log into SAM.gov. This requires a SAM user to be validated at login by having a unique code sent to a electronic device that is entered as part of the login process.
2. Restricted access to the expired registration data migrated into SAM from the Central Contractor Registration system. This prevents individuals or businesses from impersonating a legitimate business that is currently inactive.
3. When a vendor changes bank information, the parent entity is notified to reduce the risk. Parent approvals are also required if a child entity tries to register in SAM.
4. Masking sensitive data so it is not displayed publicly in the SAM database. Examples include displaying the last four characters of the Marketing Partner Identification Number TIN, ABA Routing Number, and Bank Account Number for users with approved roles.

Additionally, the OCFO sponsored training on Managing Risk Through Effective ERM. Over sixty members of the OCFO staff successfully completed the training.

GSA revamped methods to evaluate compliance with the five components and 17 principles of Internal Controls, including Principle 8, the fraud risk principle. The new tool was completed by 16 Heads of Services and Staff Offices. Fraud Risk was discussed by the GSA Senior Assessment Team, and the MCOC, to ensure it was appropriately addressed in the Administrator's Annual Statement of Assurance.

In FY 2018, the MCOC meetings included discussions on the status of corrective actions for outstanding audit findings from the annual external financial statement audit, the annual internal control plan for financial management and financial systems. At the conclusion of the fiscal year the MCOC members completed a survey to identify internal control and fraud issues not previously reported. No areas of concern were identified.

GSA addressed fraud at the program level through annual internal program reviews, which included an assessment of risk. GSA has a total of 393 internal control reviews, which it evaluates over a 5 year cycle. In FY 2018, GSA performed all 88 of the planned internal control reviews.

GSA Continues to Make Progress in Implementing Leading Practices for Managing Fraud Risk

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 now provided to the cardholder's supervisor and OHRM with a listing of aged delinquent accounts. Approving Officials (AO) conduct counsel and/or discipline employees, as necessary, in consultation with OHRM. GSA initiates salary offset for collecting 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 their travel cards, GSA uses a daily Employee Separation List and verifies the names on the list in Citibank's Citidirect Card Management System (CCMS). These accounts are immediately cancelled with Citibank. As an additional control, a monthly separation list from OHRM is used to verify closing separated employee accounts in CCMS that may have been missing from the daily list. GSA also reconciles the list of active charge card participants from Citibank to Human Resources files on a periodic basis (minimum of once per year).

Additional Travel/Purchase Card Controls

GSA program offices receive a semi-annual 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 utilizes retail blocks on questionable/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 security of an applicant's personally identifiable information.

GSA requires all charge card participants, regardless of level or responsibilities, to complete training prior to appointment or issuance of a charge card (purchase or travel).

GSA requires all approving officials, charge card holders, Agency/Organization Program Coordinators, and Charge Card Coordinators to complete charge card refresher training every two years for travel cards, and every three years for purchase cards.

Charge card program improvements in FY 2018 include:

- Monthly questionable charges and delinquency reports are sent to OHRM to ensure approving officials and/or supervisors carry out consistent application of disciplinary action, when necessary.
- Cardholder's purchase card account is suspended if a cardholder is expected to be away from the office for more than 20 business days.
- Charge Card Coordinators sample purchase card transactions monthly to ensure purchase cardholders upload supporting documentation in GSA's financial system.

GSA Utilizes 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 availability of daily transaction report. The report is then downloaded for review and verification by cardholders.

Pegasys Monthly Charge Card Transaction Report - This report is used by approving officials to review their cardholder's 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 ten days of receipt and take action on all unauthorized and questionable charges. In addition, the OAS monitors AOs' monthly reviews to ensure completion.

Questionable Charges Report - This report utilizes the MasterCard Expert Monitoring System 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; and
- Weekend and holiday transactions.

The data is reviewed and compiled into the Questionable Charges Report and sent to the AOs for review and comments.

Agency progress was also made in identifying risks and vulnerabilities to fraud with respect to payroll, beneficiary payments, large contracts, and purchase and travel cards. A new time and attendance system was implemented in the third quarter of FY 2018, which integrated leave requests with the time card, and reduced the risk associated with paying employees improperly. Controls were also strengthened to reduce the risk of paying employees after separation.

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 IPERA 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 ten 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 – This report notifies the Heads of Services and Staff Offices and Regional Commissioners of potential split transactions by cardholders. Management officials review the transactions and report to OAS on whether inappropriate use is discovered or whether charges comply with policy. Management officials are advised to counsel the employee and/or take disciplinary action in consultation with their servicing human resources office, if inappropriate use of the purchase card is discovered. Management officials must also conduct a procurement review to determine if any corrective action is needed.

Travel Card

The Questionable Charges Report described above is also utilized for travel cards. In addition, OAS uses data mining attributes such as:

- ATM transactions > \$250 in 1 Week;
- Merchant description;
- MCC;
- Merchant names;
- Returned checks; and
- Travel card transactions that are not supported by an approved travel authorization in ETS.

In FY 2018, OAS has implemented the following actions to strengthen the charge card program:

1. Monthly questionable charges reports and delinquency reports are sent to the OHRM to ensure approving officials and/or supervisors carry out consistent application of disciplinary action, when necessary.
2. Cardholder's purchase card account is suspended if a cardholder is expected to be away from the office for more than 20 business days.
3. Charge Card Coordinators perform a monthly sampling of purchase card transactions to ensure purchase cardholders upload supporting documentation in GSA's financial system.

Additional Control to Curb Fraud

The "Lost and Stolen Card Report" is 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, as warranted.

Agency progress made on establishing strategies and procedures to curb fraud included integrity awareness, OIG investigations, and the OIG hotline.

Integrity Awareness

The GSA OIG presents Integrity Awareness Briefings nationwide to educate GSA employees on their responsibilities for the prevention of fraud and abuse. This period, OIG presented 27 briefings attended by 628 GSA employees,

other Government employees, and Government contractors. These briefings explain the statutory mission of the OIG and the methods available for reporting suspected examples of wrongdoing. In addition, through case studies, the briefings make GSA employees aware of actual examples of fraud in GSA and other Federal agencies and help prevent their reoccurrence. GSA employees are the first line of defense against fraud, abuse, and mismanagement. They are a valuable source of successful investigative information.

The GSA OIG plays a significant role in the GSA's prevention and detection of fraud. The following activities were reported in the OIG Semiannual Report to Congress:

October 1, 2017 – March 31, 2018:

Significant 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 investigations that may be criminal, civil, or administrative in nature and often involve complex fraud schemes. Investigations can also involve theft, false statements, extortion, embezzlement, bribery, anti-trust violations, credit card fraud, diversion of excess Government property, and digital crimes. During the reporting period of October 1, 2017 - March 31, 2018, the office opened 54 investigative cases, closed 83 investigative cases, referred 97 subjects for criminal prosecution, and helped obtain 35 convictions. Civil, criminal, and other monetary recoveries resulting from OIG's investigations reported totaled over \$97 million.

Other Significant Work

Suspension and Debarment Initiative

GSA has a responsibility to ascertain whether the people or companies with whom it does business are eligible to participate in Federally assisted programs and are not considered "excluded parties." Excluded parties are declared ineligible to receive contracts by a Federal agency. 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.

During this reporting period, the OIG made 54 referrals for consideration of suspension or debarment to the GSA Office of Acquisition Policy. GSA issued 120 actions based on current and previous OIG referrals.

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 submit complaints using the hotline (which is also available online). OIG's first Semi-Annual Report to Congress for FY2018 documents receiving 751 hotline contracts -- 59 were referred to GSA program officials for review and appropriate action; 18 were referred to other Federal agencies; 17 were referred to the OIG Office of Audits; four were referred to the Inspections; and 59 were referred to investigative field.