Reconstruction Funds[1]

The Scenario

An auditor was requested to analyze Department of Defense (DoD) electronic disbursements of overseas construction funds. Electronic disbursements are payments made by agencies after vouchers have been approved by the contracting officer or contracting officer representative. During planning, the auditor completed the following steps:

- Reviewed relevant audit reports completed by DoD and other agency audits of electronic disbursements. The auditor focused on findings related to deficiencies in transaction data, accounting systems, and internal controls.
- When the analysis was completed, the auditor developed a spreadsheet to identify significant findings and systemic issues previously discussed in the prior audit work.
- Meetings were held with DoD officials to obtain an understanding of their disbursement processes, which varied significantly throughout the organization. The auditor used their analysis of prior audit findings and information obtained from DoD representatives to assist with completing their initial risk assessment.

To ensure the analysis was comprehensive, the auditor reviewed accessible DoD financial systems and databases. In addition to transaction data, these systems also included information on vendors and DoD employees responsible for processing the disbursement transactions. Data from other sources were also used to assist with identifying vendor and employee information anomalies, such as:

- The Excluded Parties List System. This system identifies individuals and companies that are debarred or suspended by federal government agencies from receiving federal contracts or federally approved subcontracts. A debarred or suspended individual or company is also restricted from receiving certain types of federal financial and nonfinancial assistance and benefits.
- The Central Contractor Registration database. This database is the primary contractor registry for the federal government. It collects, validates, stores, and disseminates data to support agency acquisition efforts, including federal agency contract assistance awards.
- The U.S. Postal Service's Address Aggregator. This database contains delivery point addresses and contains specialized coding which identifies characteristics of each address such as residential, commercial, P.O. Box, commercial mail facility, etc.

[1] To obtain more information on the use of forensic audit methodologies to assess electronic disbursements, refer to the Office of the Special Inspector General for Iraq Reconstruction, "Forensic Audit Methodologies Used to Collect and Analyze Electronic Disbursements of Iraq Reconstruction Funds," Report Number, SIGIR 11-006, October 23, 2010. The information in this scenario is based on information discussed in this report.

The auditor took several steps to reconcile the financial, vendor, and employee data prior to beginning their analysis of DoD electronic disbursements. For example, when reconciling vendors, they assigned a unique identifier so they could track each vendor's transactions across all disbursement funds. In some instances, single vendors were represented in the database under variations of the same name. To identify these types of vendors, the auditor removed the symbols and spaces from vendor names, and standardized abbreviations. Next, the auditor grouped and sorted the vendor names for manual confirmation. This step included assessing whether similar names should be treated as a single entity based on the name variations and addresses provided in the vendor data set.

To reconcile employee data, the auditor designed a process similar to the vendor reconciliation process. Because employee names are more standardized (i.e. there is a first and last name) than vendor names, the auditor did not complete a manual review of all employee records. However, once employee names were sorted electronically, the auditor performed some manual review for quality control purposes. As with vendors, the employee names were standardized and then assigned a unique identifier in the database so the auditor could track each employee across all disbursement funds.

The auditor then developed tests to identify anomalies that might indicate fraud or internal control weaknesses. Examples included:

- Duplicate Payments – To identify instances where a contractor may have been paid two or more times for the same invoice, work performed, and/or product delivered.
- Questionable Vendors – Identify vendor names that are generic (e.g. Cash Vendor) and vendor names that do not align with program goals.
- Payments to debarred/suspended contractors – Identify payments to debarred/suspended contractors identified in the Excluded Parties List System.
- Fictitious Addresses/High Risk Locations – Identify payment to potentially fictitious addresses and/or high risk locations or known high risk overseas banking centers.
- Notable Variances in Payment Activity – Identify payments that are outside of the norm for the vendor.

To narrow the number of electronic disbursements for review, the auditor developed a risk-scoring system based on the number and types of anomalies that were generated by their tests. Using this method, vendor and employee risk scores increased when anomalies were identified in more than one test. Next, the auditor developed another database to organize, store, analyze, and report the tests results. This database enabled the auditor to view the collective results of the anomaly tests by either vendor or by employee, and to focus on those with the highest risks scores. When testing was completed, the auditor identified over 5,000 potential fraudulent payments which were referred to DoD authorities for follow-up review.

General Comments / Lessons Learned.

Forensic auditing techniques are a valuable tool for auditors to use when analyzing large amounts of data. As illustrated in this scenario, forensic techniques can assist the auditor with identifying anomalies, trends, potential fraud, and weaknesses in internal control. As a best practice, auditors should consider including team members with forensic auditing expertise when their work requires the analysis of large amounts of financial or contracting data.

Government Auditing Standards require auditors to conduct risk assessments during audit planning. As illustrated in this scenario, prior audit work completed by DoD or other audit agencies often provide valuable information that can assist auditors in their assessment of audit risk. Other sources of information may also include work completed by independent public accounting firms, academic studies, or research conducted by professional accounting or auditing organizations. Review of work completed by other organizations also helps the auditor to identify systemic problems.

FRAUD INDICATORS

- **Review of the Excluded Parties List System discloses individuals or companies that are debarred or suspended by federal government agencies from receiving federal contracts or federally approved subcontracts.**

- **Contractor is not registered in the Central Contractor Registration database.**

- **Comparison of contractor addresses to the U.S. Postal Service Address Aggregator identifies suspect addresses such as residential, P.O. Box, or commercial mail facilities.**

- **Contractor is paid two or more times for the same invoice, work performed, and/or product delivered.**

- **Vendor has a generic name or the vendor name does not align with program goals.**

- **Payments are made to high risk locations, known high risk overseas banking centers, or outside of the norm for a vendor.**

- **Forensic auditing techniques disclose a large number of anomalies occurring among vendors and/or employees receiving, or processing, electronic payments.**