OFFICE OF THE SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION

FORENSIC AUDIT METHODOLOGIES USED TO COLLECT AND ANALYZE ELECTRONIC DISBURSEMENTS OF IRAQ RECONSTRUCTION FUNDS

SIGIR 11-006
OCTOBER 28, 2010

SIGIR

Special Inspector General for IRAQ Reconstruction

October 28, 2010

FORENSIC AUDIT METHODOLOGIES USED TO COLLECT AND ANALYZE ELECTRONIC DISBURSEMENTS OF IRAQ RECONSTRUCTION FUNDS

Summary of Report: SIGIR 11-006

Why SIGIR Is Issuing This Report

Public Law 108-106, as amended, requires the Special Inspector General for Iraq Reconstruction (SIGIR) to prepare a final forensic audit report on all funding appropriated for the reconstruction of Iraq. To address part of this requirement, SIGIR developed forensic audit methodologies to assess electronic disbursements of Iraq reconstruction funds. These are the payments made after contractor vouchers have been approved. SIGIR is conducting additional tests to assess whether the vouchers submitted for payment are reasonable, allowable, and allocable; and this methodology will be reported in a separate report.

The electronic disbursement methodologies combine automated data mining procedures with standard audit and investigative techniques to detect questionable transactions and develop evidence for use in administrative actions or civil or criminal fraud prosecutions. Much of our methodology was developed from lessons learned from audits of Iraq reconstruction projects and criminal investigations.

SIGIR is issuing this report to provide Inspectors General and agency managers with information on our methodologies that may be of use in conducting similar forensic audit activities.

This report is being issued as a nonaudit service as defined by Generally Accepted Government Auditing Standards. Therefore, this report contains no recommendations.

SIGIR's Methodology

SIGIR used a two-phase approach to analyze electronic disbursements of reconstruction funds by the Department of Defense (DoD), the Department of State (DoS), and the U.S. Agency for International Development (USAID). In phase one, we collected data from agency financial systems and prepared it for testing. To do this, we:

- identified the transactions to be tested and the primary agencies responsible for the transactions
- collected data on relevant contractor and U.S. government employees associated with the transactions
- reconciled and validated the transactions to the extent possible

Altogether, we were able to collect and reconcile180, 000 transactions totaling about $39.76 billion. All of these transactions were from the four major reconstruction funds: the Iraq Relief and Reconstruction Fund ($19.83 billion), the Iraq Security Forces Fund ($14.1 billion), the Economic Support Fund ($1.83 billion), and the Commander's Emergency Response Program ($4.0 billion).

Our data on relevant contractors and government employees associated with the transactions was derived from agency financial systems such as the Corps of Engineers Financial Management System, and DoD's Deployable Disbursing System.

In phase two, we tested the transactions to identify anomalies that might indicate internal control weaknesses or possible fraud. SIGIR auditors and investigators collaboratively designed 10 anomaly tests to analyze the transactions. Our tests included looking for payments to contractors that had been debarred or suspended, contractors with fictitious addresses, contractors with questionable names, and transactions that violated separation of duty principles. All of our tests are discussed in the body of this report.

To further narrow our list of transactions we also developed a risk-scoring system based on the number and type of anomalies generated by our tests. When vendors and employees had anomalies in more than one test then their risk scores would rise. This allowed SIGIR auditors and investigators to focus on the vendors and government employees that potentially were the highest risk.

Lastly, we developed a database to organize, store, and report the results of our anomaly tests. The database enables us to view the collective results of the anomaly tests by either vendor or by government employee and to focus on those with the highest risk scores. The data is organized into "cases" which combine transactions identified by the anomaly test sets for each vendor or employee by fund and agency financial system.

For more information, contact SIGIR Public Affairs at (703) 428-1100 or PublicAffairs@sigir.mil

SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION

October 28, 2010

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF STATE
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
AUDITOR GENERAL, DEPARTMENT OF ARMY
INSPECTOR GENERAL, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT
INSPECTOR GENERAL, SPECIAL INSPECTOR GENERAL FOR AFGHANISTAN RECONSTRUCTION

SUBJECT: Forensic Audit Methodologies Used To Collect and Analyze Electronic Disbursements of Iraq Reconstruction Funds (SIGIR 11-006)

The report provides technical information on some of the methodologies used by the Special Inspector General for Iraq Reconstruction's (SIGIR) to meet its mandate for a final forensic audit report on all funds deemed to be amounts appropriated or otherwise made available for Iraq relief and reconstruction activities. We developed these methodologies in accordance with our statutory responsibilities contained in Public Law 108-106, as amended, which also incorporates the duties and responsibilities of inspectors general under the Inspector General Act of 1978. These audit methodologies were developed for SIGIR Projects 9005, 9012, and 9013.

SIGIR is issuing this information report as a nonaudit service as defined by Generally Accepted Government Auditing Standards to provide Inspectors General and agency managers with information on our methodologies that may be of use in conducting similar forensic audit activities.

We appreciate the courtesies extended to the SIGIR staff. For additional information on the report, please contact Glenn D. Furbish, Assistant Inspector General for Audits (Washington, DC), (703) 604-1388/ glenn.furbish@sigir.mil or Jason Venner, Principal Deputy Assistant Inspector General for Audits (Washington, DC), (703) 607-1346/ jason.venner@sigir.mil.

Stuart W. Bowen, Jr.
Inspector General

cc: U.S. Secretary of State
U.S. Secretary of Defense
Administrator, U.S. Agency for International Development

Table of Contents

Forensic Audit Methodologies Used To Collect and Analyze Electronic Disbursements of Reconstruction Funds

SIGIR 11-006 **October 28, 2010**

Introduction

Public Law 108-106, as amended, requires that the Special Inspector General for Iraq Reconstruction (SIGIR) prepare a final forensic audit report on all funding appropriated for the reconstruction of Iraq To address part of this requirement, we developed forensic audit methodologies to assess electronic disbursements of Iraq reconstruction funds. Electronic disbursements are payments made by agencies after vouchers have been approved by the contracting officer or contracting officer representative. SIGIR is conducting additional tests to assess whether vouchers submitted for payment are reasonable, allowable, and allocable and this methodology will be reported in a separate report.

SIGIR's electronic disbursement methodologies combine automated data mining procedures with standard audit and investigative techniques to detect questionable transactions and develop evidence for use in administrative actions or civil or criminal fraud prosecutions. SIGIR is issuing this report to provide Inspectors General and agency managers with information on our methodologies that may be of use in conducting similar forensic audit activities. This report is being issued as a nonaudit service as defined by Generally Accepted Government Auditing Standard A3.03b.[1]

Background

SIGIR's electronic disbursement methodologies were applied only to U.S. funds appropriated or made available for Iraq reconstruction, which total about $53.79 billion as of July 2010. Of this amount, SIGIR focused its efforts on about $47.28 billion appropriated or made available to the Departments of Defense (DoD) and State (DoS) and the U.S. Agency for International Development (USAID).[2] All of the funds reviewed came from the four major Iraq reconstruction funds: the Iraq Relief and Reconstruction Funds I and II (IRRF), the Iraq Security Forces Fund (ISFF), the Commander's Emergency Response Program (CERP), and the Economic Support Fund (ESF).

Pursuant to SIGIR's congressional mandate, we collected and analyzed nearly 180,000 DoD, DoS, and USAID expenditure transactions. The total value of the transactions was about $39.76 billion, which represents approximately 84% of the appropriations or funds made available to these

[1] *Government Auditing Standards: July 2007 Revision*, GAO-07-731G, July 2007.
[2] About $6.51 billion appropriated to other reconstruction funds and agency operating accounts were outside the scope of the forensic audit and were not tested.

agencies from the four major funds and about 75% of the total appropriated or made available for Iraq reconstruction. Table 1 provides the total amount analyzed by fund and by agency.

Table 1—Value of Expenditures Tested for FYs 2003 through 2009 (in billions)

Fund	Amount Appropriated	DoD	DoS	USAID	Total Tested	Percent of Appropriation Tested
IRRF I & IRRF II	$20.86	$13.78	$1.64	$4.41	**$19.83**	**95%**
ISFF	18.04	14.10	0.0	0.0	**14.10**	**78%**
ESF	4.56	0.0	0.23	1.60	**1.83**	**40%**
CERP[a]	3.82	4.00	0.0	0.0	**4.00**	**105%**
Total	**$47.28**	**$31.88**	**$1.87**	**$6.01**	**$39.76**	

Notes:

[a] CERP funds are not appropriated, but rather have generally been authorized from DoD's Operations and Maintenance account. The discrepancy between the amount authorized and what SIGIR reviewed is discussed later in this report.

Source: SIGIR, Quarterly Report to the United States Congress, 7/30/2010, and SIGIR analysis of agency data.

To develop our methodology and gain an understanding of the controls over the expenditure of funds, we reviewed relevant prior SIGIR audit reports and other agency audits of the funds. We concentrated on findings related to deficiencies in transaction data, accounting systems, and internal controls. The most common finding was poor contract oversight, especially for interagency contracts. Two examples are one agency contracting with a third party to manage another agency's contracts, and contracts between agencies to provide services. Another deficiency was a lack of adequate internal controls over payments. Table 2 summarizes 14 SIGIR audits and the control weaknesses identified.

Table 2—Control Weaknesses Found by SIGIR in Major Reconstruction Contract Audits

SIGIR Audit Report	Excessive numbers of task and change orders	High contracting official turnover or inadequate staffing	Construction deficiencies not tracked/remedied	Inadequate contractor oversight	Inadequate subcontractor oversight	Inadequate accounting for property or inventory	Inadequate reviews of contractor invoices	Invoices and other documents missing or in disarray	Contract billing weaknesses, risk of erroneous billings
07-009		✓			✓		✓		
07-016		✓		✓			✓	✓	
08-004					✓	✓			✓
08-010		✓							✓
08-011		✓						✓	
08-018				✓					
08-019	✓	✓	✓			✓		✓	
09-003		✓		✓			✓		
09-008		✓							
09-010							✓	✓	
09-014	✓			✓				✓	
09-017			✓						
09-021							✓	✓	
09-026								✓	
TOTAL	**2**	**7**	**2**	**4**	**2**	**2**	**5**	**7**	**2**

Source: SIGIR audit reports as of 10/28/2009.

SIGIR also examined findings from other agency audits. For example, a DoD Inspector General audit dated May 22, 2008, concluded that the U.S. Army did not maintain adequate internal controls over commercial payments and that DoD did not maintain a complete audit trail over $134.8 million in CERP payments.[3] This research contributed to our planning.

Finally, we met with agency officials to gain an understanding of their disbursement processes. These processes sometimes varied within agencies. For example, DoS' bureau field offices in U.S. embassies overseas process invoices and payments within their own designated systems.

[3] *Internal Controls Over Payments Made in Iraq, Kuwait and Egypt*, Report Number D-2008-098, May 22, 2008.

Objectives

SIGIR's objectives for this report are to present the methodologies used to collect and analyze data for electronic disbursements of Iraq reconstructions funds.

Data Collection Methodologies

SIGIR collected data from agency financial systems and prepared this data for testing while maintaining data integrity. We developed a work plan that included identifying (1) the funds to be included for testing, (2) the agencies that expended the funds, and (3) the vendors and individuals associated with the transactions. We then reconciled the data we obtained from the various agency systems and other sources to the extent possible to prepare it for analysis.

Data Sources

To ensure that our analyses were comprehensive, we looked at all agency financial systems and databases that contained relevant data. DoD has several systems that include detailed or summary transaction data, including the Corps of Engineers Financial Management System (CEFMS), Deployable Disbursing System (DDS), and Computerized Accounts Payable System (CAPS). USAID's transaction data is in its Phoenix system, and DoS' transaction data is in its Global Financial Management System (GFMS) and, for transactions processed overseas, in individual bureau systems at U.S. Embassies. In addition to transaction data, these systems also contain information on vendors and U.S government employees associated with the transactions. Table 3 provides detail on which systems were tested, organized by agency and the relevant fund(s).

Table 3—System Tested by Fund and Data Owner

Data Owner	DoD			USAID	DoS
	USACE[a]	DFAS[b]			
Fund/System	**CEFMS**	**DDS**	**CAPS[c]**	**Phoenix**	**GFMS**
IRRF	X	X	X	X	X
CERP[d]	X	X	X		
ISFF	X				
ESF				X	X

Notes

[a] U.S. Army Corps of Engineers.

[b] Defense Finance and Accounting Service.

[c] Computerized Accounts Payable System.

[d] CERP payments were often in cash, and the transaction data was entered into the electronic systems afterwards.

Source: SIGIR, as of 9/30/2010.

In addition, we obtained data from other sources to assist with testing for vendor and employee information anomalies. These include:

- The Excluded Parties List System (EPLS). This system identifies individuals and companies 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. EPLS collects both current and archived entities that have been excluded from doing business with the federal government.

- The Central Contractor Registration (CCR) database. CCR is the primary contractor registry for the federal government. CCR collects, validates, stores, and disseminates data to support agency acquisition efforts, including federal agency contract and assistance awards. According to the Federal Acquisition Regulation 4.11, CCR registration is required before the federal government can award a contract (although there are exceptions to this requirement including international registrants and contracts supporting contingency operations).
- The U.S. Postal Service's Address Aggregator. This database contains delivery point addresses serviced and contains specialized coding that identifies characteristics of each address such as identifying it as residential, commercial, P.O. Box, commercial mail facility, etc.

Challenges in Collecting Data

We encountered several challenges while collecting data from DoS and USAID that affected the scope of our work. Some of these challenges included the following:

- DoS and USAID data systems record expenditures not only for contracts but also for grants and cooperative agreements. Grants can be provided either directly to a nongovernmental organization or through transfers of funds to other federal agencies, which then use the funds to provide grants to NGOs. If grants are made directly to nongovernmental organizations that information is recorded in DoS' GFMS and USAID's Phoenix systems. However, if money is transferred to another agency to award grants, only the name of the U.S. government agency, not the name of the grant recipient, is recorded in the systems.
- DoS' GFMS does not record and save historical information on individuals involved in its transactions. According to a DoS official, only the last individual to touch a transaction is identified in GFMS; individuals previously involved in the transactions are not recorded or maintained in the system. As a result, complete information on employees associated with DoS transactions is not available.
- DoS' GFMS does not include the vendor code and vendor name for overseas transactions. Instead, it contains generic names based on the vendor type, such as employee or non-government vendor, and the location of the post processing the transaction. Information on the actual vendor paid is maintained overseas at the post and is not available in GFMS.
- USAID's Phoenix does not contain data on transactions data prior to 2006 because the data was maintained in another financial system and was not migrated to Phoenix.

Data Reconciliation

SIGIR took several steps to reconcile the financial, vendor, and employee data prior to our analysis. We cross-checked the financial data with U.S. Treasury account numbers that indicate the type of funds or major purpose of the appropriation. We worked with system owners to determine the possible cause for variances and obtained additional data when necessary.

Our primary difficulty was in reconciling and validating CERP transactions. The CERP transaction data that DoD provided included other funds and/or CERP funds used in Afghanistan. This was caused by discrepancies in how some transactions were coded in DoD financial systems. Because we could not specifically identify all Iraq-related CERP transactions, we included all CERP transaction data in our analysis. As a result, the amount of CERP transactions analyzed ($4.0 billion) as shown above in Table 1 is greater than the amount DoD reports as allocated for Iraq ($3.82 billion).

To reconcile vendors, we assigned each vendor a unique identifier so that we could track each vendor's transactions across all funds. Our primary challenge was that, in some cases, single vendors are represented in the database under variations of the same name. To identify these cases, we removed the symbols and spaces from vendor names, and standardized abbreviations. We then electronically grouped and sorted the vendor names for manual confirmation. This entailed 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, we 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 we did not conduct a complete manual review of all employee records. However, once employee names were sorted electronically, we performed some manual review for quality control purposes. It is noted most of the names analyzed were U.S. government employees associated with Iraq reconstruction transaction data. As with vendors, the employee names were standardized and then assigned a unique identifier in our database so that we could track each employee across all funds.

Data Analysis Methodologies

SIGIR ran a series of tests to identify anomalies that might indicate fraud and/or internal control weaknesses. To do this, SIGIR auditors and investigators collaboratively designed 10 anomaly tests to assess each transaction. To further narrow our list of transactions we also developed a risk-scoring system based on the number and type of anomalies generated by our tests. Vendor and employee risk scores would increase when anomalies were identified in more than one test. Last, we developed a database to organize, store, and report our anomaly test results. The database enables us to view the collective results of the anomaly tests by either vendor or by employee and to focus on those with the highest risk scores.

Development of Anomaly Tests

To develop the list of anomaly tests, SIGIR auditors and investigators collaboratively assessed SIGIR audit reports, audit reports from other agency Inspectors General, and past criminal investigations. Throughout the process SIGIR auditors and investigators continually refined our anomaly tests and added additional tests as necessary. These tests are designed to enable us to determine the legitimacy of a transaction and whether improper expenditures are attributable to administrative error or fraud. Table 4 details the tests we performed to check for anomalies in the electronic transactions.

Table 4—Anomaly Tests and Intended Results

Anomaly Test	**Intent of Test**
Duplicate payments	Identify instances where it appears 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 appear to align with the program goals
Notable variances in payment activity	Identify payments outside of the "norm" for a vendor
Invoice date analysis	Identify payments occurring prior to or on the date of invoice and sequentially-numbered contractor invoices
Payments to debarred/ suspended contractors	Identify payments to debarred/suspended contractors identified in the Excluded Parties List System
Separation of duties	Identify breakdowns in separation of duties whereby the same government contracting official originates the request for payment, approves the request, is the payer and/or payee
Fictitious addresses/High Risk Locations	Identify payments to possibly fictitious addresses and/or high risk locations or known high-risk banking centers such as Cyprus and Beirut
Payee Validation	Identify payments to debarred/suspended contractors who are also an Approver or Originator
Fictitious contractors	Identify payments to contractors with no associated D-U-N-S[a]/CAGE[b] number
Application of Benford's Law[c]	Identify nonrandom transaction amounts to identify instances a contractor submitted false invoices using false invoice totals

Notes:

[a] The Data Universal Numbering System or D-U-N-S® Number is Dunn and Bradstreet's copyrighted, proprietary means of identifying business entities on a location-specific basis. This unique nine-digit identification number has been assigned to over 100 million businesses worldwide. The D-U-N-S® Number was incorporated into the Federal Acquisition Regulation in April 1998 as the Federal Government's contractor identification code for all procurement-related activities.

[b] A Commercial and Government Entity (CAGE) Code is a five-character code that identifies companies doing or wishing to do business with the Federal Government.

[c] Benford's law states that the leading digit in lists of numbers from many real-life sources of data is distributed in a non-uniform way. Accordingly, the first digit is 1 almost one third of the time, and subsequent digits occur as the first digit in descending frequency, where 9 is the leading digit less than one time in twenty.

Source: SIGIR analysis as of 09/30/2010.

We also developed sub-tests for each primary test to identify variations of anomalies and possible fraud schemes. See Appendix A for a detailed listing of the primary tests and sub-tests performed by fund and agency financial system.

Duplicate Payments

The purpose of our duplicate payments test was to identify transactions where (1) a vendor was paid two or more times for the same invoice/work performed, and (2) different vendors were paid for the same service. To identify these transactions, we searched the data for the following:

- transactions with the same transaction date (either invoice date or payment date, depending on fields available), dollar amount, vendor ID/name, obligation number, delivery order number, and line item number

- transactions with the same transaction date (either invoice date or payment date, depending on fields available), dollar amount, and vendor ID/name, but different obligation
- transactions with the same transaction date (either invoice date or payment date, depending on fields available) and dollar amount, but different obligation and vendor ID/name
- transactions with the same dollar amounts, but different obligation, vendor ID/name and transaction dates

Only check and EFT transactions were tested.

Questionable Vendor

The purpose of our questionable vendor test was to identify transactions where (1) no vendor was identified, and (2) payments were made to possibly fictitious vendors. To identify these transactions we searched the data for the following:

- transactions where the vendor name was "cash" or contained the word "cash"
- transactions where the vendor name was "vendor" or contained the word "vendor"
- transactions where the vendor name field was not populated, (i.e. blank vendor names)
- transactions where the vendor name was generic
- transactions where the vendor name did not align with the purpose of the fund

Once the questionable transactions were identified, SIGIR then compiled vendor addresses for each transaction and searched the Central Contractor Registration (CCR) database for a record of the name. If a vendor was in the CCR, SIGIR attempted to match the address recorded in the CCR to the address provided in the transaction record. SIGIR also conducted internet searches to locate vendor websites and attempted to match the address provided in the vendor record to the website, or other third party source. Additionally, SIGIR used existing vendor websites to establish the nature of the business to determine if it aligned with the purpose of the fund.

Notable Variances in Payment Activity

The purpose of the notable variances in payment activity test was to identify payments out of the expected range for a specific vendor based on payments over the time of an obligation. SIGIR performed four tests in this area. First, we calculated an average net monthly payment dollar amount by obligation number. Months with payment totals for an obligation that were more than 2.5 standard deviations removed from the average net monthly payment amount for an obligation were identified by this test.[4]

We also the same test described above but excluded the calculation by obligation number. Instead, we calculated the average net monthly payment dollar amount by that vendor ID for transactions that did not include an associated obligation number in the data fields and was not contract specific. Similar to the test that calculated by obligation number, months with payment totals to a

[4] When dealing with variance in a population, 2.5 standard deviations approximately represents the top 1% of a normal distribution. The goal of the variance rule is to focus on the highest dollar amounts in a population. Using 2.5 standard deviations is a standard benchmark for segmenting the population, even though transaction data tends not to follow a normal distribution.

vendor that were more than 2.5 standard deviations removed from the average net monthly payment amount for a vendor were identified by this anomaly test.

Third, we identified potential changes in payments for a vendor. This test was created based on information from a prior investigation that the payment amount was subtly increased during the contract term in order to allow the paying agent to withhold a portion of the cash. The test identified specific transactions that were outside of the average payment range for a given vendor. SIGIR calculated the average net monthly payment dollar amount by each vendor. Any transactions by a vendor that were more than 2.5 standard deviations removed from the average payment amount for that vendor were identified by this anomaly test.

Last, we identified vendors and employees with a related gap in transaction activity. The test first identified vendors with a gap in transactions of at least six months. Additionally, the vendor had to have at least five transactions prior to the gap in activity and at least five transactions after the gap in activity. Once we identified the population of vendors with a discontinuous timeframe of transactions, we identified the employees involved in the various roles in these transactions. The timeframe of the vendor gap in activity was then compared to the timeframe of the transactions for that employee across vendors. If the timeframe of the gap in activity for the employee completely matched the gap in activity for a vendor we selected both the vendor and employee for additional review.

Invoice Date Analysis

The purpose of our invoice date analysis test was to identify transactions that met certain criteria related to the timing of the invoices and payments. For example, payments are not typically made prior to or on the same day that services are performed or goods are received, nor are payments usually made on weekends and holidays. To identify transactions with unusual payment patterns, SIGIR looked for the following:

- transactions where payments were made prior to the invoice date
- transactions where payments were made on the invoice date
- transactions where payment were made on a weekend or holiday

Payments to Debarred and Suspended Contractors

The purpose of our debarred and suspended contractors test was to determine if payments were made to contractors who are listed in the U.S. government's Excluded Parties List System (EPLS). This test identified payments made to debarred/suspended contractors, prior to debarment, during debarment, and after debarment.[5] We compiled a broad list of vendor name variations from the transaction data and compared it to the EPLS list. We also took steps to ensure the names were spelled consistently, and conducted a "wildcard match" that compared the vendor list to the EPLS list for situations where either the vendor name from the transaction data was a part of the EPLS name and vice versa. SIGIR then manually examined the results for potential false positives. Vendor names initially matched to the EPLS list that were determined to be different entities than those listed on the EPLS were removed from the results.

[5] The government can terminate a contract as soon as they become aware that the contractor was debarred or suspended but is responsible for paying the contractor for services performed up to the date of termination.

We also identified transaction time periods for vendors identified as potential matches in the EPLS list. The transaction time period was then compared to the debarred/suspended timeframe to determine how the transactions lined up with the debarment/suspension.

Separation of Duties

The purpose of our separation of duties test was to identify potential collusion between employees, and employees and vendors. Tests were aimed at identifying potential separation of duties weaknesses for the following functions:

- Obligation Originator
- Obligation Approver
- Invoice Creator
- Invoice Receiver
- Receipt Voucher Certifier

The Deployable Disbursing System (DDS) has different employee functions than the other systems. For DDS, we tested separation of duties for the following functions:

- Voucher creator
- Voucher certifier
- Voucher payer
- Voucher modifier

Additional tests detected instances where:

- the same individual performed multiple functions for one transaction
- an employee involved in a transaction had the same name as the vendor paid
- employees were paired together for transactions very frequently (100% of the time) or very infrequently (less than 0.5% of the time)

These later tests were designed to identify possible cases of collusion.

Finally, we developed a test specifically designed to analyze separation of duties related to CERP transactions. Separation of duties is an internal control requiring more than one person to complete a task such as requesting a payment, approving the payment, and making the payment. We then manually checked against agency records to ensure that improper payments had not been made.

Fictitious Addresses/High Risk Locations

The purpose of our tests for fictitious and questionable addresses was to determine if payments were sent to invalid addresses, addresses located in high risk international locations, or to other suspicious addresses.

SIGIR searched the following types of addresses:

- Commercial Mail Receiving Agencies—private mailboxes
- Residential
- Invalid Address
- High-Risk International Location
- Prison/Detention Facility Address

When a vendor address was identified as Invalid, Residential, High-Risk International Location, or a prison/detention facility we searched the CCR database for a record of the vendor name. If a name was found, we attempted to match it with the address recorded in the vendor data. We also conducted internet searches for vendor websites and instances of the vendor name and recorded address.

Payee Validation

The purpose of our payee validation test was to determine if employees involved in the transactions also appeared in the EPLS. SIGIR compared the employee lists we gathered to the EPLS for potential matches based on the first and last names of employees. The results were then manually analyzed for potential false positives. For example, if the first and last names were the same, but the middle initial was different, this would result in a false positive.

Fictitious Contractors

The purpose of our fictitious contractor tests was to ensure that all vendors receiving payments were legitimate companies. We compared vendor names and their Commercial and Government Entity (CAGE) codes[6] to the names and CAGE codes in the CCR database to identify conflicting information. When the data conflicted we compared the vendor name in the CCR record to the vendor name provided in the testing data. Those that were identified as exact name matches were not further tested. Those that were identified as having a potentially different name were then researched in the online CCR database for further information. For the vendors with CAGE codes that could not be located in the contractor registry data extract, we performed a further search for the vendor's registration/CAGE code in the CCR online database in an effort to reconcile the vendor with a CCR record. We could not perform these tests when the systems did not include CAGE codes. This sometimes occurs because foreign companies and U.S.-based companies performing work related to a contingency operation do not have to have CAGE code. We retained these transactions for possible further review.

Application of Benford's Law

The purpose of our Benford's Law tests was to identify non-random transaction amounts. Benford's Law states that in lists of naturally occurring numbers from many (but not all) sources of data, the first digit is distributed in a specific, non-uniform way. According to this theory, the first digit is 1 almost one-third of the time, and larger digits occur as the leading digit with lower and lower frequency where 9 as a first digit occurs less than one time in 20. We ran this test

[6] A Commercial and Government Entity (CAGE) Code is a five-character code that identifies companies doing or wishing to do business with the Federal Government.

electronically on the population of transaction data for systems with more than 10,000 transactions—CEFMS, CAPS, and DDS—to identify transactions which fell out of the Benford's pattern. To help identify transactions with potentially higher risks, we ran Benford's Law on transaction amounts across all vendors, as well as transaction amounts pertaining to each vendor. We then combined the results from these two tests and created a more focused list of 1-digit and 2-digit numbers to flag transactions for further review.

Risk Scoring

We developed a risk-scoring system to prioritize the list of vendors and employees for further analysis. For each test, we assigned vendors and employees a risk score based on the number and type of anomaly they generated when the anomaly tests were run against the electronic transaction data. Similarly, each sub-test was assigned a risk score. For example, when vendors and employees had anomalies in more than one sub-test within the same test set, then the vendor's/employee's risk score for that those anomaly tests would be set at the highest sub-test risk score.[7] By summing the maximum risk score received for each primary test, a total risk score was accumulated for each vendor and employee specific to the fund and agency system. Risk scores ranged from 0 through 10 for vendors and 7 through 15 for employees. Table 5 lists the maximum possible risk score for each primary anomaly test.

[7] The one exception for the separation of duties test was for employee. Due to the nature of the test, for this instance the sub-tests which tested the employee pairing received a separate aggregated score, and that score was added to the overall employee case risk score.

Table 5—Maximum Possible Risk Score for Anomaly Test Set

Test Set	Vendor Maximum Score	Employee Maximum Score
Payments to Debarred/Suspended Contractors	10	n/a
Fictitious Address/High Risk Locations	10	n/a
Questionable Vendor	9	n/a
Separation of Duties	9	15
Duplicate Payments	7	n/a
Fictitious Contractors	7	n/a
Invoice Date Analysis	7	7
Notable Variances in Payment Activity	5	n/a
Application of Benford's Law	1	n/a
Debarred and Suspended Employees	0	10

Note:
n/a = not applicable
[a] Test was only applicable to CERP/DDS, IRRF/DDS, and CERP/CAPS testing.

Source: SIGIR analysis of agency data as of 9/30/2010.

Managing and Reporting Anomaly Test Results

SIGIR developed a customized database to organize, store, and report the results of our anomaly tests. The Case Management Tool (CMT) was designed to enable SIGIR to view the collective results of the anomaly tests by either vendor or by government employee and to focus on those with the highest risk scores. We organized data into "cases" which combined transactions identified by the anomaly test for each vendor by fund and system.[8] Vendors and employees were assigned an overall case score based on the total risk score for the tests for the vendor and employee tests within the specific fund and system. For example, if a vendor had IRRF and ISFF transactions in CEFMS and IRRF transactions in Phoenix, we opened three distinct cases for that vendor: one case for IRRF-CEFMS-identified transactions, one case for ISFF-CEFMS-identified transactions, and one case for IRRF-Phoenix-identified transactions. Case scores were used to manage the transactions and test results by vendor and employee.

The CMT provides information by cases on the overall statistics of transactions involving the vendor or employee, and the details of the individual anomaly test results. Various tabs within the database provided different levels of information. The CMT enables SIGIR to view and analyze the following types of information:

- variations of vendor names and addresses
- statistics on the total number of transactions for the vendor or employee and the total dollars paid

[8] "Cases" in the CMT do not indicate whether an audit or investigation had been opened on the organization or individual.

- statistics by month on transactions and total dollars paid
- summary of anomaly tests
- risk score calculation for the case
- listing of anomaly tests and key information
- viewing of transactions by anomaly tests, by month, or all for a vendor/employee

The CMT provides various options for viewing the transactions for a given vendor or employee. For example, transactions could be viewed by associated anomaly test. Additionally, the CMT provides the ability to select different criteria and view transactions meeting those criteria, such as those occurring within a certain month. The CMT also has the built-in capability to produce reports for specific vendors or employees, including overall statistics as well as details of relevant transactions. These results can be exported into Microsoft Excel for further analysis.

Appendix A—Anomaly Test List by Fund and System

Table 11—Anomaly Primary and Sub-Tests Listed by Fund and Financial System

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Duplicate Payments	Same obligation no/vendor/date/ amount	√	√	√	√	√	√	√	√	√	√
Duplicate Payments	Same vendor/date/amount	√	√	√	√	√	√	√	√	√	√
Duplicate Payments	Same date/amount	√	√	√	√	√	√	√	√	√	√
Duplicate Payments	Same amount	√	√	√	√	√	√	√	√	√	√
Payments to Debarred/ Suspended Contractors	Exact match to EPLS	√	√	√	√	√	√	√	√	√	√
Payments to Debarred/ Suspended Contractors	Wildcard match to EPLS	√	√	√	√	√	√	√	√	√	√

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Fictitious Contractors	Vendor Name does not agree with CCR	√	√	√		√	√		√		√
Fictitious Contractors	Cage Code not found in CCR	√	√	√		√	√		√		√
Questionable Vendors	Vendor Name is "Cash"	√	√	√	√	√	√	√	√	√	√
Questionable Vendors	Vendor Name is "Vendor"	√	√	√	√	√	√	√	√	√	√
Questionable Vendors	Vendor Name is blank	√	√	√	√	√	√	√	√	√	√
Questionable Vendors	Vendor Name is questionable	√	√	√	√	√	√	√	√	√	√
Notable Variances in Payment Activity - Monthly Payment	Monthly activity profiling - by obligation number	√	√	√	√	√	√	√	√	√	√

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Notable Variances in Payment Activity - Monthly Payment	Monthly activity profiling - by each vendor							√	√		
Notable Variances in Payment Activity – Discontinuous Timeframe	Vendors with discontinuous timeframe of transactions/payments.							√	√		
Notable Variances in Payment Activity - Average Payment	Changes in average payment over time							√	√		
Separation of Duties	Obligation Approver = Obligation Originator = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Obligation Originator = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Obligation Approver = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Obligation Approver = Obligation Originator	√	√	√	√		√		√	√	

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties	Obligation Approver = Obligation Originator - 100% Pairing	√	√	√	√		√		√	√	
Separation of Duties	Obligation Approver = Obligation Originator - < 0.5% Pairing	√	√	√	√		√		√	√	
Separation of Duties	Invoice Creator = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Authorized Receiver = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Receipt Voucher Certifier = Vendor	√	√	√	√		√		√	√	
Separation of Duties	Receipt Voucher Certifier = Obligation Originator	√	√	√	√		√		√	√	
Separation of Duties	Receipt Voucher Certifier = Obligation Approver	√	√	√	√		√		√	√	

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties	Receipt Voucher Certifier = Invoice Creator	√	√	√	√		√		√	√	
Separation of Duties	Receipt Voucher Certifier = Authorized Receiver	√	√	√	√		√		√	√	
Separation of Duties	Obligation Originator = Invoice Creator = Authorized Receiver	√	√	√	√		√		√	√	
Separation of Duties	Obligation Approver = Invoice Creator = Authorized Receiver	√	√	√	√		√		√	√	
Separation of Duties	Obligation Originator = Obligation Approver = Invoice Creator = Authorized Receiver	√	√	√	√		√		√	√	
Separation of Duties	Authorized Receiver = Receipt Voucher Certifier - 100% Pairing	√	√	√	√		√		√	√	

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties	Authorized Receiver = Receipt Voucher Certifier - < 0.5% Pairing (Ratio based on Authorized Receiver, not Receipt Voucher Certifier)	√	√	√	√		√		√	√	
Separation of Duties - DDS	Create User = Vendor							√			
Separation of Duties - DDS	Certifier User = Vendor							√			
Separation of Duties - DDS	Paid User = Vendor							√			
Separation of Duties - DDS	Modify User = Vendor							√			
Separation of Duties - DDS	Create User = Certifier User = Vendor							√			

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties - DDS	Create User ID = Certifier User ID							√			
Separation of Duties - DDS	Certifier User = Paid User							√			
Separation of Duties - DDS	Certifier User = Modify User							√			
Separation of Duties - DDS	Paid User = Modify User							√			
Separation of Duties - DDS	Create User = Certifier User = Paid User							√			
Separation of Duties - DDS	Create User = Certifier User = Modify User							√			
Separation of Duties - DDS	Create User = Paid User = Modify User							√			

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties - DDS	Certifier User = Paid User = Modify User							√			
Separation of Duties - DDS	Create User = Certifier User = Paid User = Modify User							√			
Separation of Duties - DDS	Create User and Certifier User - 100% Pairing							√			
Separation of Duties - DDS	Create User and Certifier User - < 0.5% Pairing							√			
Separation of Duties - DDS	Certifier User and Paid User - 100% Pairing							√			
Separation of Duties - DDS	Certifier User and Paid User < 0.5% Pairing							√			

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Separation of Duties - DDS	Vendor and Create User - 100% Pairing Vendor and Obligator/Pay Agent Relationship: Vendor always has same person acting as Create User.							√			
Separation of Duties - DDS	Vendor and Certifier User - 100% Pairing Vendor and Obligator/Pay Agent Relationship: Vendor always has same person acting as Certifier User.							√			
Separation of Duties - DDS	Vendor and Paid User - 100% Pairing Vendor and Obligator/Pay Agent Relationship: Vendor always has same person acting as Paid User.							√			
Separation of Duties	Generic User ID = Create User or Certifier User or Paid User or Modifier User							√	√		
Fictitious Addresses/High Risk Locations	International addresses - Vendors in high risk international location	√	√	√	√	√	√	√	√	√	√

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Fictitious Addresses/High Risk Locations	U.S. addresses – Commercial Mail Receiving Agencies addresses	√	√	√	√	√	√	√	√	√	√
Fictitious Addresses/High Risk Locations	U.S. addresses - Residential/Apartment	√	√	√	√	√	√	√	√	√	√
Fictitious Addresses/High Risk Locations	U.S. addresses - PO Box search	√	√	√	√	√	√	√	√	√	√
Fictitious Addresses/High Risk Locations	U.S. addresses - Invalid (Vacant or Inaccurate Address)	√	√	√	√	√	√	√	√	√	√
Fictitious Addresses/High Risk Locations	U.S. addresses - Prison address	√	√	√	√	√	√	√	√	√	√
Fictitious Addresses/High Risk Locations	No Street information for an International Address	√	√	√	√	√	√	√	√	√	√
Application of Benford's Law	First Digit Benford's Analysis	√	√								

Test Set	Sub-test Description	ISFF CEFMS	IRRF CEFMS	IRRF CAPS	IRRF PX[a]	IRRF GFMS	CERP CEFMS	CERP-IRRF DDS	CERP CAPS	ESF PXa	ESF GFMS
Application of Benford's Law	First 2 Digits Benford's Analysis	√	√					√	√		
Invoice Date Analysis	Invoice Date is after the Transaction Date	√	√	√	√	√	√		√	√	√
Invoice Date Analysis	Invoice Date is the same as the Transaction Date	√	√	√	√	√	√		√	√	√
Invoice Date Analysis	Transaction Dates on a Weekend or Holiday	√	√			√	√				√
Debarred/ Suspended Employees	Exact and Wildcard Match to EPLS	√	√	√	√		√	√	√	√	

[a] Px = Phoenix, the USAID transactional database system.

Source: SIGIR analysis of agency data as of 9/30/2010.

Appendix B—Acronyms

Acronym	Description
CAGE	Commercial and Government Entity Code
CAPS	Computerized Accounts Payable System
CCR	Central Contractor Registration
CEFMS	Corps of Engineers Financial Management System
CERP	Commander's Emergency Response Program
CMT	Case Management Tool
DDS	Deployable Disbursing System
DFAS	Defense Financial Accounting Service
DoD	Department of Defense
DoS	Department of State
EFT	Enhanced File Transfer
EPLS	Excluded Parties List System
ESF	Economic Support Fund
FY	Fiscal Year
GFMS	Global Financial Management System
IRRF	Iraq Relief and Reconstruction Fund
ISFF	Iraq Security Forces Fund
SIGIR	Special Inspector General for Iraq Reconstruction
USACE	U.S. Army Corps of Engineers
USAID	U.S. Agency for International Development

Appendix C—Forensic Audit Team Members

This report was prepared and the forensic audit conducted under the direction of Glenn D. Furbish, Assistant Inspector General for Audits, Office of the Special Inspector General for Iraq Reconstruction.

The following SIGIR staff members are participating in the forensic audit effort and contributed to this report:

William F. Bedwell

David Childress

Benjamin H. Comfort

Adam T. Hatton

Donald V. McNamara

Richard C. Newbold

Dennis W. Rader

Robin L. Rowan

George S. Salvatierra

Robert A. Whiteley

Contract support for this effort provided by Deloitte Consulting LLP

Appendix D—SIGIR Mission and Contact Information

SIGIR's Mission	Regarding the U.S. reconstruction plans, programs, and operations in Iraq, the Special Inspector General for Iraq Reconstruction provides independent and objective: • oversight and review through comprehensive audits, inspections, and investigations • advice and recommendations on policies to promote economy, efficiency, and effectiveness • deterrence of malfeasance through the prevention and detection of fraud, waste, and abuse • information and analysis to the Secretary of State, the Secretary of Defense, the Congress, and the American people through Quarterly Reports
Obtaining Copies of SIGIR Reports and Testimonies	To obtain copies of SIGIR documents at no cost, go to SIGIR's Web site (www.sigir.mil).
To Report Fraud, Waste, and Abuse in Iraq Relief and Reconstruction Programs	Help prevent fraud, waste, and abuse by reporting suspicious or illegal activities to the SIGIR Hotline: • Web: www.sigir.mil/submit_fraud.html • Phone: 703-602-4063 • Toll Free: 866-301-2003
Congressional Affairs	Hillel Weinberg Assistant Inspector General for Congressional Affairs Mail: Office of the Special Inspector General for Iraq Reconstruction 400 Army Navy Drive Arlington, VA 22202-4704 Phone 703-428-1059 Email hillel.weinberg@sigir.mil
Public Affairs	Deborah Horan Director of Public Affairs Mail: Office of the Special Inspector General for Iraq Reconstruction 400 Army Navy Drive Arlington, VA 22202-4704 Phone: 703-428-1217 Fax: 703-428-0817 Email: PublicAffairs@sigir.mil