



SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION

January 28, 2011

LETTER FOR DIRECTOR, ARMY BUDGET, OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT and COMPTROLLER).

SUBJECT: Interim Report: Action Needed To Address Missing Iraq Transaction Data (SIGIR 11-008)

This interim report addresses the Special Inspector General for Iraq Reconstruction's (SIGIR) concerns over missing Iraq transaction data and it seeks your assistance in recovering the data. The missing data has been reported to the Army Financial Management Command and Defense Finance and Accounting Service (DFAS) by the Department of Defense Inspector General (DoDIG). While the Army Financial Management Command took some steps to reconstruct the missing data, these efforts have not been fully successful.

SIGIR is primarily concerned about the missing data because Section 3001, (o)(2), of Public Law 108-106, as amended requires us to prepare a final forensic audit report on all amounts appropriated or otherwise made available for the reconstruction of Iraq, and this data is necessary for us to fulfill our Congressional mandate. Additionally, a substantial amount of the data could be cash transactions made through the Commander's Emergency Response Program (CERP), which prior SIGIR audits and investigations have shown to be vulnerable to fraud and theft. Further, reconstructing the missing data should be important to the Department of the Army because (1) the missing data likely includes Personally Identifiable Information (PII) from pay agents and other U.S. military personnel that could be used to defraud these individuals; and (2) the missing data may include classified information.

Background

In December 2008, SIGIR announced an audit of Department of Defense (DoD) appropriation, obligation, and expenditure data related to Iraq relief and reconstruction projects (Project 9005). We are performing this analysis to meet our mandate to forensically audit all Iraq reconstruction funds. In collecting the records, we found that about \$2.5 billion in transactions, primarily CERP transactions, were recorded in the Deployable Disbursing System (DDS).

DFAS developed DDS in 2005 to serve as an on-site, tactical disbursing system for deployed military units. The system runs on individual computers that operate independently of a central network or server and enables DoD personnel to maintain accountability of appropriated funds in the field. When units return from the field, the data is to be transferred into DFAS' primary financial system. SIGIR's objective for this report is to determine the extent to which DoD has attempted to retrieve transaction data missing from DDS and evaluate the sensitivity of missing data and follow-up steps it must take to address missing data.

Transaction Data Is Missing

During the course of our data collection process, we reconciled the DDS data we were provided with Congressional appropriations and other DoD financial system data and found that some DDS data was missing. We questioned DFAS and the Army Financial Management Command about the missing data in early 2010, and these officials told us that the DoDIG had already made them aware of the situation. According to an Army Financial Management Command official, the missing transaction data is from two sites in Iraq under SIGIR's forensic review; Camp Speicher, Tikrit, for the period October 2005 through March 2007, and Camp Liberty, Baghdad, for the period October 2005 through August 2006.

An Army Financial Management Command official told us that the data is missing because of a computer malfunction and because some DDS users did not follow the appropriate procedures. The official said that computers have a limited data storage capacity, and when a computer hard drive reaches capacity, units are directed to transfer data from the hard drive to portable electronic media, such as compact disks or an external hard drive. The data is then to be transferred into DDS' main system for archiving, as soon as possible thereafter. In one instance in which data is missing, a unit transferred its data to another computer. That computer's hard drive crashed, and the data was lost. In another instance, units transferred their data to disks but did not complete the transfer of the data to the DDS main system. The units reportedly brought the data home when they left Iraq and subsequently lost the disks. The DoDIG made recommendations to address this problem¹, and in April 2009, new procedures were established governing the handling and storage of data.

The Missing Data Is Needed To Meet SIGIR's Forensic Mandate

SIGIR's interest in the missing data is to satisfy our forensic audit mandate as well as to address concerns that the loss may represent an intentional breach of CERP internal controls. Prior SIGIR work has shown significant problems with controls over CERP, particularly for cash disbursements made through the program. DoD personnel in Iraq are responsible for handling the money, creating paper records, and entering the transactions into DDS to record the payments. While some of these duties may be segregated, the risk of DoD personnel colluding on criminal acts is heightened because the entire disbursement process is handled at the local level. To date, SIGIR investigations have resulted in six convictions of DoD personnel involving CERP-related payment activities.

The total amount of information that is missing cannot be determined without reconstructing the activity through a review of each voucher. In an effort to evaluate the scope of the missing data, SIGIR collected DDS data associated with the Camp Liberty disbursing site for September 2006 through May 2007. We found that the average monthly payment activity for this period was approximately \$75 million, and 96% of the transactions were in cash for CERP projects. While this average cannot be directly related to the missing transaction data, it suggests that the missing data contains a substantial amount of payment activity.

As of December 2010 the missing data has not been reconstructed. According to a DFAS official, the Army would be responsible for reconstructing the data because it controls database

¹ *Internal Controls Over United States Marine Corps Commercial and Miscellaneous Payments Processed Through the Deployable Disbursing System*, D-2010-037, 1/25/2010.

security in the field, to include physical security of its computers and portable data storage. This DFAS official noted that, during the time period in question, there was no central DDS repository in DFAS, and the Army was responsible for policy and procedures concerning the archiving and purging of data and subsequent safekeeping of the data. This official added that the propriety of any payment was the responsibility of the disbursing officer for the specific DSSNs. According to an Army Financial Management Command official, attempts were made to locate the missing data by contacting the units responsible for managing the records. However, this effort was unsuccessful because, in many cases, personnel operating the DDS sites had changed due to units rotating in and out of Iraq, and no records of the portable media were maintained in Iraq. According to a DFAS official, all paper copies of transactions were sent to DFAS Rome, New York for reconciliation with the monthly accountability statement. This official added that it is possible to reconstruct the missing transaction data using paper records associated with the transactions.

Sensitive and Classified Information May Have Been Lost

While the missing data is of concern to SIGIR because of our forensic audit mandate, it is likely that the missing data also contains Personally Identifiable Information (PII) of military members and may also include classified information.

SIGIR's review of DDS data has found that it includes the names of military and civilian personnel responsible for making payments of Iraq reconstruction funds. DoD's *Guidance on Protecting PII (August 2006)* requires that all PII information be evaluated for impact of loss or unauthorized disclosure and protected accordingly. For example, any collection of electronic records stored on a single device containing PII on more than 500 people is to be encrypted. However, according to a DFAS official, archived data in the 2006 and 2007 time period was not encrypted. Federal laws and Office of Management and Budget guidance² also require agencies to develop policies and procedures, and implement a notification process if PII information is lost. In determining whether notification is required, this guidance instructs agencies to assess the potential for harm due to a breach by considering the risk factors of the data. DoD implemented these procedures, but the Army Financial Management Command has not assessed the circumstances of the breach to determine whether notification of impacted personnel is required.

It is also possible that classified information is included in the missing data. In 2009, the DoDIG reported³ that DoD personnel had entered classified information into two unclassified DoD systems, one of which was DDS. Therefore, it is possible that the missing DDS data from 2006 and 2007 may contain classified information, such as the names of intelligence sources, which could expose the sources and their associates to considerable risk. As with PII, existing DoD

² Federal Information Security Management Act of 2002, 44 USC § 3541, Privacy Act of 1974, 5 USC § 552a, and *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Office of Management and Budget M-07-16, 05/22/2007.

³ *Identification of Classified Information in Unclassified DoD Systems During the Audit of Internal Controls and Data Reliability in the Deployable Disbursing System*, D-2009-054, 2/17/2009.

guidance⁴ requires that known or suspected instances of unauthorized public disclosure of classified information are to be reported promptly and investigated to decide the nature and circumstances of the disclosure. To date, the Army Financial Management Command has not determined whether classified information was included in the missing DDS data or whether this information was disclosed.

According to a DFAS official, during the time frame in question, the DDS Program Management Office was not aware of any sensitive data being processed in DDS. This official added that, subsequent to this time period, and with the development of the repository, all historical data has been through a cleansing process and all new data goes through a similar review process prior to importing to the repository.

Conclusions, Recommendation, and Management Comments

Conclusions

The missing DDS data prevents SIGIR from meeting its mandate to forensically audit Iraq reconstruction funds. The fact that the missing data involves high risk cash transactions from CERP also raises SIGIR's concern.

Moreover, unless these records are reconstructed, the Army cannot determine whether PII and classified information was lost. Determining whether PII and classified information is missing is necessary to mitigate any potential consequences resulting from the loss of this information.

Recommendations

SIGIR recommends that the Director, Army Budget, Office of the Assistant Secretary of the Army (Financial Management and Comptroller) direct the Army Financial Management Command to

1. Reconstruct all missing transactions by using available DFAS records, and provide this information to SIGIR.
2. Review the reconstructed transactions to determine whether they include any PII and classified information, and take appropriate action pursuant to federal law and applicable guidance.

Management Comments and Audit Response

In written comments on a draft of this report, the Army concurred with the report's conclusions and recommendations. Comments are reprinted in their entirety in Appendix D. While the Army concurred with the draft report, SIGIR identified some areas of the written response that required clarification. For example, the Army noted that "An ongoing DOD IG audit previously identified this electronic information gap and determined that the loss represented less than one one-hundredth of a percent of the total DDS payments for the period..." SIGIR contacted a DOD IG official associated with the ongoing audit for verification. The DOD IG official told

⁴ Directive 5210.50 *Unauthorized Disclosure of Classified Information to the Public*, Department of Defense, 7/22/2005.

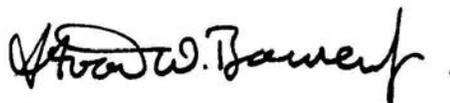
SIGIR that the data they identified as missing from DDS was based on a limited review. They added that it is not possible to determine the percentage missing until the hard copy payment vouchers are fully reconciled to DDS data."

In addition, the Army indicated in its response that, since any missing data was encrypted and password-protected, it was unnecessary to locate vouchers associated with the data in an effort to determine whether it contained PII or classified information. However, we were told by DFAS officials with knowledge of DDS in Iraq that transaction data during the time period in question was not encrypted. Consequently, we believe action should be taken by the Army to rule out the possibility of PII or classified data spillage.

In addition to written comments from the Army, SIGIR also received technical comments from DFAS and modified the report as appropriate.

- - - -

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 Nancee Needham, Deputy Assistant Inspector General for Audits (Baghdad), (240) 553-0581 ext. 3793/ nancee.needham@iraq.centcom.mil.



Stuart W. Bowen, Jr.
Inspector General

cc: Commander, U.S. Central Command
Commanding General, U.S. Forces-Iraq
Director, Defense Finance and Accounting Service

Appendix A—Scope and Methodology

In December 2008, the Special Inspector General for Iraq Reconstruction (SIGIR) initiated Project 9005 to meet, in part, a Congressional mandate to forensically audit the Department of Defense's (DoD) management of funds appropriated for the reconstruction of Iraq. SIGIR is required to prepare a final forensic audit of these pursuant to Public Law 108-106 and periodically issues interim reports, such as this report (Project 9005c), to keep the Congress informed of the results of our ongoing efforts. Our reporting objective is to determine the extent to which DoD has attempted to retrieve transaction data missing from DDS and evaluate the sensitivity of missing data and follow-up steps it must take to address missing data. We performed the audit under authority of Public Law 108-106, as amended, which also incorporates the duties and responsibilities of inspectors general under the Inspector General Act of 1978. SIGIR conducted this particular review from March 2010 to December 2010.

To accomplish our objective we obtained DDS transaction data from the Department of Defense. We reconciled this information with Congressional appropriations and other DoD financial systems that maintained similar information to ensure the data we were provided was accurate and complete. Our analysis showed that data was likely missing from the DDS. We then held discussions with officials from the Army Financial Management Command and the Defense Finance and Accounting Service, who confirmed that DDS data was missing. We reviewed the Army's internal controls processes and procedures to oversee and manage DDS data to determine if there were weaknesses in their system of controls. Last, we obtained and reviewed guidance from the Office of Management and Budget and DoD to determine what action should be taken, if any, when DoD loses control of Personally Identifiable Information and classified data.

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Use of Computer-processed Data

This report discusses difficulties SIGIR encountered in utilizing DDS data to respond to its Congressional mandate to prepare a final forensic audit report on all amounts appropriated or otherwise made available for the reconstruction of Iraq. During the course of our data collection process, we reconciled the DDS data we were provided with Congressional appropriations and other DoD financial system data and found that some DDS data was missing.

Internal Controls

We reviewed Army internal controls to oversee, manage, and secure DDS data. Specifically, SIGIR identified and assessed internal controls the Army used in managing portable electronic

storage devices and sensitive transaction data. The results of the review are presented in this report.

Prior Coverage

We reviewed the following reports issued by SIGIR and the Department of Defense, Office of the Inspector General:

SIGIR

Forensic Audit Methodologies Used To Collect and Analyze Electronic Disbursements of Iraq Reconstruction Funds, SIGIR 11-006, 10/28/2010.

Iraq Reconstruction Funds: Forensic Audits Identifying Fraud, Waste, and Abuse – Interim Report #5, SIGIR 11-005, 10/28/2010.

Iraq Reconstruction Funds: Forensic Audits Identifying Fraud, Waste, and Abuse – Interim Report #4, SIGIR 10-019, 7/26/2010.

Iraq Reconstruction Funds: Forensic Audits Identifying Fraud, Waste, and Abuse – Interim Report #3, SIGIR 10-017, 4/28/2010.

Iraq Reconstruction Funds: Forensic Audits Identifying Fraud, Waste, and Abuse – Interim Report #2, SIGIR 10-011, 1/28/2010.

Iraq Reconstruction Funds: Forensic Audits Identifying Fraud, Waste, and Abuse – Interim Report #1, SIGIR 10-004, 10/28/2009.

Department of Defense, Office of the Inspector General

Internal Controls Over United States Marine Corps Commercial and Miscellaneous Payments Processed Through the Deployable Disbursing System, D-2010-037, 1/25/2010.

Identification of Classified Information in Unclassified DoD Systems During Audit of Internal Controls and Reliability in the Deployable Disbursing System, D-2009-054, 2/17/2009.

Internal Controls Over Payments Made in Iraq, Kuwait and Egypt, D-2008-098, 5/22/2008.

Appendix B—Acronyms

Acronym	Description
CERP	Commander's Emergency Response Program
DDS	Deployable Disbursing System
DFAS	Defense Finance and Accounting Service
DoD	Department of Defense
PII	Personally Identifiable Information
SIGIR	Special Inspector General for Iraq Reconstruction

Appendix C—Audit Team Members

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

The staff members who conducted the review and contributed to the report include:

Adam Hatton

Richard Newbold

Appendix D—Management Comments



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
FINANCIAL MANAGEMENT AND COMPTROLLER
109 ARMY PENTAGON
WASHINGTON DC 20310-0109

Special Inspector General for Iraq Reconstruction
Attention: Glenn D. Furbish,
Assistant Inspector General for Audits
400 Army Navy Drive
Arlington, Virginia 22202

Dear Mr. Furbish:

This office has reviewed the Special Inspector General for Iraq Reconstruction (SIGIR) interim report entitled "Action Needed to Address Missing Deployable Disbursing System [DDS] Data (SIGIR 11-008)." The report concludes that "missing DDS data prevents SIGIR from meeting its mandate to forensically audit Iraq reconstruction funds." In addition, the report recommends the Director of the Army Budget direct the Army Financial Management Command to (1) "reconstruct all missing transactions ... and provide this information to SIGIR" and (2) "review the reconstructed transactions to determine whether they include any PII [personally identifiable information] and classified information"

The Department of the Army concurs with comment on the interim report's conclusion and recommendations. While SIGIR is correct that a very small amount of the electronic collection of DDS data was lost, the hard copy of the data remains readily available for audit. Consequently, there is no requirement to "reconstruct" the transactions and create an electronic version. An ongoing DoD IG audit previously identified this electronic information gap and determined that the loss represented less than one one-hundredth of a percent of the total DDS payments for the period and that hard copy documents supporting these payments were on file at DFAS-Rome. Typically, the hard copy documents from individual cash payments contain greater detail than the DDS data. Given the minute percentage of "missing" voucher data and absence of the detailed individual cash payment information it would have contained, the loss should have no material impact on the outcome of the audit and a review of the available hard copy documentation should provide even better information for audit purposes.

The SIGIR interim report also makes the statement "... it is likely that the missing data also contains Personally Identifiable Information of military members and may also include classified information." The Department asserts that this is a correct but misleading statement. Based on our analysis, all data would have been encrypted and password-protected, such that risk of any unauthorized disclosure would be minimal at best. In addition, while a previous audit did identify classified information in one DDS database from a single location during a single period of time, further extensive reviews of all DDS databases failed to detect additional instances of classified data being input to

the system, even when contained in hard-copy supporting documents. As such, it is highly improbable that the "missing" data contained any classified information.

The preceding comments notwithstanding, the Department of the Army recognizes that electronic copies of the DDS data enhances visibility and the ability to audit. Consequently, the Army Financial Management Command and DFAS have already instituted several procedures to minimize the risk of losing electronic data in the future. In addition, DFAS is in the process of scanning all DDS documents to create an electronic reference library. They expect to complete this project in late 2012 or early 2013. To complete its audit, SIGIR may wait for the DFAS project to be completed, may request copies of selected documentation on file in hard copy, or may review any or all of the hard copy documents maintained at DFAS-Rome.

The point of contact in this office is LTC Gina Shaunette, (703) 614-3253 (DSN 224-3253), gina.shaunette@conus.army.mil.

Sincerely,



David C. Coburn
Colonel, US Army
Director of Management & Control

Appendix E—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
Office 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
