United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at
1 p.m.
Monday,
September 28, 1998

FINANCIAL MANAGEMENT

Improvements Needed in Air Force Vendor Payment Systems and Controls

Statement of Jeffrey C. Steinhoff
Director of Planning and Reporting
Accounting and Information Management Division

GAO/T-AIMD-98-308

Summary

The two cases of Air Force vendor payment fraud discussed in this testimony resulted from a weak internal control environment. As discussed in our report that is being released today, the lack of segregation of duties and other control weaknesses, such as weak controls over remittance addresses, created an environment where employees were given broad authority and the capability, without compensating controls, to perform functions that should have been performed by separate individuals under proper supervision. Similar internal control weaknesses continue to leave Air Force funds vulnerable to fraudulent and improper vendor payments.

For example, as of mid-June 1998, over 1,800 Defense Finance and Accounting Service (DFAS) and Air Force employees had a level of access to the vendor payment system that allowed them to enter contract information, including the contract number, delivery orders, modifications, and obligations, as well as invoice and receiving report information and remittance addresses. No one individual should control all key aspects of a transaction or event without appropriate compensating controls. This level of access allows these employees to submit all the information necessary to create fraudulent or improper payments. In addition, the automated vendor payment system is vulnerable to penetration by unauthorized users due to weaknesses in computer security, including inadequate password controls.

Further, DFAS lacked procedures to ensure that the date that invoices were received for payment and the date that goods and services were received were properly documented. These are critical dates for ensuring proper vendor payments and compliance with the Prompt Payment Act, which requires that payments made after the due date include interest.

Our report on these issues details a number of recommendations to help improve the controls over Air Force vendor payments. Until DFAS and the Air Force complete the actions to address control weaknesses in vendor payment systems and processes and maintain accountability over goods and services received, Air Force funds will continue to be vulnerable to fraudulent and improper vendor payments.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in this important hearing to discuss the current status of internal controls over the process for Air Force vendor payments. Your request that we review this issue was prompted by two recent fraud cases involving vendor payments made on behalf of the Air Force. As discussed in our report to you that is being released today,[1] the lack of segregation of duties and other control weaknesses, such as weak controls over remittance addresses, created an environment where employees were given broad authority and the capability, without compensating controls, to perform functions that should have been performed by separate individuals under proper supervision. Today, similar internal control weaknesses continue to leave Air Force funds vulnerable to fraudulent and improper vendor payments.

Effective internal controls are essential to achieving the proper conduct of government business with full accountability for the resources made available. Internal controls serve as the first line of defense for preventing and detecting fraud and help ensure that an agency meets its missions, goals, and objectives; complies with laws and regulations; and is able to provide reliable financial and other information concerning its programs, operations, and activities.

Over the years, we and Defense auditors have issued a number of reports that have pointed to serious internal control weaknesses in the Department of Defense's (DOD) payment processes and systems. In part, because of the seriousness of these problems and other related problems, we identified DOD's contract payment process as error prone and costly and designated DOD contract management as a high-risk area.[2] In this regard, we have reported that serious internal control weaknesses have resulted in numerous erroneous and, in some cases, fraudulent payments.[3] For example, $3 million in fraudulent payments were made to a former Navy supply officer on over 100 false invoices.[4]

[1]Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

[2]High-Risk Series: An Overview (GAO/HR-95-1, February 1995), High-Risk Series: Defense Contract Management (GAO/HR-95-3, February 1995), and High-Risk Series: Defense Contract Management (GAO/HR-97-4, February 1997).

[3]DOD Procurement: Millions in Overpayments Returned by DOD Contractors (GAO/NSIAD-94-106, March 14, 1994) and Funds Returned by DOD Contractors (GAO/NSIAD-98-46R, October 28, 1997).

[4]Financial Management: Status of Defense Efforts to Correct Disbursement Problems (GAO/AIMD-95-7, October 5, 1994).

Also, we have identified computer security as a governmentwide high-risk area. With respect to DOD, in May 1996, we reported[5] that unknown and unauthorized individuals are increasingly attacking highly sensitive unclassified information on DOD's computer systems, which we found were particularly susceptible to attack through Internet connections.

Summary of Two Fraud Cases

Against this backdrop of long-standing concerns with DOD's internal controls over its payment processes, I would like to briefly outline the specifics of the two recent fraud cases. The first case involved fraudulent activity between October 1992 and February 1993 related to two Bolling Air Force Base (AFB) office automation contracts resulting in an embezzlement of over $500,000.[6] The Bolling AFB contracting officer's technical representative (COTR) had authority to authorize, approve, verify, and process contract and payment documentation and receive and accept goods and services. In addition, this person was not adequately supervised. The COTR's supervisor told investigators and us that she allowed the COTR to perform these duties independently without close supervision. The COTR was able to embezzle over $500,000 by creating fictitious invoices and receiving reports.

The COTR was able to accomplish this scheme without detection by Air Force officials because he took advantage of his broad authority and the lack of adequate supervision. In addition, at the time of this incident, the address on the invoice was used as the remittance address, which is a control weakness. Therefore, directing the payments to himself was simply a matter of listing his post office box as the contractor address on the false invoices.

Authorities were only alerted to the COTR's embezzlement when he attempted to withdraw a large portion of the funds, and suspicious bank officials put a hold on the accounts and notified the U.S. Secret Service. After coming under suspicion, the COTR prepared a letter stating that overbilling errors had been made and returned the funds to the government. Following an investigation by the Air Force Office of Special Investigation, the COTR pleaded guilty and was sentenced to 3 years

[5]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

[6]GAO's Office of Special Investigations issued a separate report on contractor activities associated with the Bolling AFB contract fraud entitled, DOD Procurement Fraud: Fraud by an Air Force Contracting Official (GAO/OSI-98-15, September 23, 1998).

probation and ordered to pay $495. Further details on the COTR's schemes can be found in GAO/OSI-98-15.

We also were unable to determine whether the Air Force received the goods and services paid for under the two Air Force contracts associated with the Bolling AFB fraud because, in addition to missing records—another indicator of a weak internal control environment—a number of improper procedures were followed for receipt and control of equipment and services paid for under the contracts. For example, the COTR had also directed the contractor to falsify invoices and receiving reports by changing the type and quantity of items received under a delivery order.

The second case covered fraudulent activities of a Staff Sergeant between October 1994 and June 1997 at two locations resulting in a $435,000 embezzlement and attempted theft of over $500,000. The first known location where fraudulent payments were made was Castle AFB, California, between October 1994 and May 1995. The Staff Sergeant, who was Chief of Material in the Accounting Branch, had broad access to the automated vendor payment system, which allowed him to enter contract information, including contract numbers, delivery orders, modifications, and obligations, as well as invoice and receiving report information and remittance addresses. The Staff Sergeant used this broad access to process invoices and receiving report documentation that resulted in eight fraudulent payments totaling $50,770 that were identified. The invoices prepared by the Staff Sergeant designated the name of a relative as the payee and his own mailing address as the remittance address, although any address, including a post office box, could have been used. Castle AFB closed in September 1995, and the Staff Sergeant was transferred to the Defense Finance and Accounting Service (DFAS) operating location at Dayton, Ohio.

At DFAS Dayton, the Staff Sergeant was assigned as the Vendor Pay Data Entry Branch Chief in the Vendor Pay Division. As Vendor Pay Chief, the Staff Sergeant was allowed a level of access to the vendor payment system similar to the access he previously held at Castle AFB. Between November 1995 and January 1997, the Staff Sergeant prepared false invoices and receiving reports that resulted in nine fraudulent payments totaling $385,916. By designating the remittance address on the false invoices, the Staff Sergeant was able to direct fraudulent payments to an accomplice.

In February 1997, the Staff Sergeant was reassigned to DFAS Dayton's Accounting Branch and his access to the vendor payment system was removed. However, while assigned to the Accounting Branch, the Staff Sergeant created two false invoices totaling $501,851 and submitted them for payment in June 1997, using the computer password of another DFAS employee who had a level of access comparable to that previously held by the Staff Sergeant.

The Staff Sergeant's fraudulent activities were detected when, for an invoice totaling $210,000, an employee performing a reconciliation identified a discrepancy between the contract number associated with the invoice in the vendor payment system and in the accounting system. These two numbers should always agree. For this invoice, the Staff Sergeant failed to ensure that the contract cited was the same in both systems. Further research determined that the contract was not valid and the payment was fraudulent. A second fraudulent invoice for $291,851, the $50,770 in fraudulent payments at Castle AFB, and the $385,916 in fraudulent payments at DFAS Dayton were detected during the subsequent investigation of the DFAS Dayton fraud.

The Staff Sergeant was convicted of embezzling over $435,000 and attempted theft of over $500,000. He was also convicted of altering invoices and falsifying information in the vendor payment system—a violation of 18 U.S.C. 1001[7]—to avoid interest on late payments and improve reported performance for on-time payments, which is discussed later in this testimony. In July 1998, the Staff Sergeant was sentenced to 12 years imprisonment. The Dayton case also involved the altering of invoices to improve reported payment performance, thereby depriving government contractors of interest payments.

Continuing Internal Control Weaknesses in Air Force Vendor Payment Processes

Now, Mr. Chairman, I would like to turn our attention to the current control environment at the locations where these incidents occurred. Our work shows that similar internal control and system weaknesses continue to leave the Air Force vulnerable to fraudulent or improper vendor payments.

For example, as of mid-June 1998, over 1,800 DFAS and Air Force employees had a level of access to the vendor payment system that allowed them to enter contract information, including the contract

[7]Under 18 U.S.C. 1001, knowingly and willfully falsifying or concealing a material fact in relation to any matter within the jurisdiction of an executive agency or department of the United States government is a criminal offense, punishable by fine, 5 years in prison, or both.

number, delivery orders, modifications, and obligations, as well as invoice and receiving report information and remittance addresses. In addition, the automated vendor payment system is vulnerable to penetration by unauthorized users due to weaknesses in computer security, including inadequate password controls. Finally, controls over remittance addresses remain a weakness.

Access to Vendor Payment System Remains a Serious Vulnerability

An August 1996 Air Force Audit Report[8] disclosed that DFAS personnel did not properly control access to the vendor payment system and recommended that DFAS review and reduce vendor payment system access levels where appropriate. Our review of vendor payment system access levels as of mid-June 1998 showed that across DFAS and Air Force installations, individual users could enter contract data, including obligations, and invoice and receiving report information, and change remittance addresses for vendor payments. Currently, there are four access levels to the vendor payment system: inquiry, clerk, subsupervisor, and supervisor. Inquiry is read only access. Clerk access allows the user to enter data other than remittance addresses. Subsupervisor access allows the user to input or change contract data; information on obligations, invoices, and receiving reports; and remittance addresses. Supervisor access allows the user to perform all subsupervisor functions as well as assign or remove access. The Staff Sergeant who committed the DFAS Dayton fraud had supervisor access.

Proper and effective internal controls would preclude allowing any individual user to have the ability to record an obligation, create and change invoices and receiving reports, and enter remittance addresses. Our review of the vendor payment process at DFAS Dayton and DFAS Denver's Directorate of Finance and Accounting Operations confirmed that employees with supervisor and subsupervisor access to the vendor payment system could make fraudulent payments without detection by entering contract information and obligations, invoice and receiving report data, and changing or creating a remittance address. If the data on a false invoice and receiving report match the information on the voucher, certifying officers are not likely to detect a fraudulent payment through their certification process, a key prevention control.

Second, problems with the lack of segregated access within the payment system application are compounded by the excessive and widespread

[8]Air Force Audit Agency Project 96054010: General and Application Controls Within the Integrated Accounts Payable System (August 1, 1996).

access to the system throughout DFAS and the Air Force. Our review of vendor payment system access levels as of mid-June 1998 showed that 1,867 users across DFAS and Air Force installations had supervisor or subsupervisor access. Further, 94 of these users had not accessed the system since 1997, indicating that they may no longer be assigned to vendor payment operations. In addition, 171 users had not accessed the system at all, possibly indicating that access is not required as a regular part of their duties. DFAS officials told us they were unaware that such a large number of employees had broad access to the vendor payment system.

After we briefed the DFAS Denver Center Director about our concerns, he told us that the current operational review program would be revised to place a greater focus on internal controls, including the review of vendor payment system access levels. DFAS officials told us that for Air Force employees outside the operating locations who had supervisor or subsupervisor access, but only need status reports, they have initiated action to reduce the level of access to inquiry only. They also told us that they would consider modifying the supervisor and subsupervisor access levels across DFAS locations to provide for greater segregation of duties within the vendor payment application for employees responsible for processing payments.

Finally, with respect to access controls, there are significant weaknesses in the mainframe operating system security and the vendor payment system application that would allow unauthorized users to make fraudulent or improper payments. A recently completed review by the Defense Information Systems Agency (DISA), performed at our request, identified the following problems with the mainframe operating system on which DFAS Denver's Directorate of Finance and Accounting Operations vendor payment system runs.

- Excessive access to powerful system utilities was permitted. These utilities enable a user to access and manipulate any data within the mainframe computer and vendor payment system.
- Routine system monitoring and oversight was not performed to identify and follow-up on user noncompliance with security standards. This allowed serious security weaknesses, which are commonly exploited by hackers, to exist. For example, default passwords, which are commonly known, were not disabled. Further, passwords and user IDs were not managed according to DISA policies. For example, 12 users, including a

security administrator, had passwords that were set to never expire, exceeding the 90-day DISA policy.

In addition, our tests of the local network and communication links to the DFAS Denver Directorate of Finance and Accounting Operations and the DFAS Dayton vendor payment systems showed that these systems are vulnerable to penetration by unauthorized internal DFAS and Air Force users. For example, because vendor payment system passwords and user IDs are transmitted across the local network and communication links in clear text, readily available software would permit any user to read vendor payment system passwords and user IDs.

Inadequate Controls Over Remittance Addresses

The ability to misdirect payments to a personal post office box or to an accomplice's address was a major factor in the two fraud cases. Again, we found that weaknesses in controls over remittance addresses remain. Although DFAS changed its policy in April 1997 to require that the contractor address listed in the contract be used as the remittance address, it still permits the use of the invoice address if the invoice states that payment must be made to a specified address. This continues to afford a mechanism to misdirect payments for fraudulent purposes. This problem is compounded by the widespread access to the vendor payment system, just discussed, that allows users to enter changes to the remittance address.

The Defense Logistics Agency has an initiative under way intended to validate remittance addresses. Under the Central Contractor Registry,[9] contractors awarded a contract on or after June 1, 1998, are required to be registered in order to do business with the government. While DFAS Denver Center officials did not have a target date for full implementation of the Registry, they expect that 80 percent of the eligible contracts will be included in the Registry by mid-1999.

The Registry, which is accessed through the Internet using a password or manually updated using a standard form, is intended to ensure that the contractor providing payment data, including the remittance address, is the only one authorized to change these data. However, this process, while an improvement, still has vulnerabilities related to control over remittance address changes. First, as previously discussed, DOD's computer systems are particularly susceptible to attack through connections on the Internet. In addition, once the addresses are downloaded from the Registry to the

[9]The Registry will not cover grants, awards, utilities, legal claims, or claims for household goods.

vendor payment system, they will be vulnerable to fraudulent or improper changes due to the access control weaknesses previously discussed. Therefore, Registry controls over the remittance addresses will only be effective to the extent that access to remittance addresses currently held by DFAS and Air Force employees is eliminated or compensating controls are implemented.

DFAS Dayton Control Environment Permitted Circumvention of Prompt Payment Act Provisions

As I stated before, the Dayton case also involved the altering of invoices—a violation of 18 U.S.C. 1001—to improve reported payment performance, thereby depriving government contractors of interest payments. Again, we found that although some improvements have been made, today's control environment would still permit such activity at most DFAS locations. Specifically, DFAS lacks procedures to ensure that the date that invoices were received for payment and the date that goods and services were received were properly documented. These are critical dates for ensuring proper vendor payments and compliance with the Prompt Payment Act,[10] which requires that payments made after the due date include interest.

The falsification of payment documentation to improve reported performance for on-time payments undermined DFAS Dayton's internal controls over payments and impaired its ability to detect or prevent fraud. This was done by (1) altering dates on invoices received from contractors, (2) replacing contractor invoices with invoices created using an invoice template that resided on DFAS Dayton personal computers used by vendor payment employees, and (3) throwing away numerous other invoices.

According to DFAS internal review and Air Force investigative reports, during 1996, DFAS Dayton also altered faxed invoices to change invoice receipt dates to avoid late payment interest required by the Prompt Payment Act. Not only did this practice undermine late payment controls, but an environment in which altered documents are commonplace made it more difficult to detect other fraudulent activity, such as the false invoices generated for personal financial gain.

Our review of selected fiscal year 1997 DFAS Dayton and DFAS Denver's Directorate of Finance and Accounting Operations vendor payment transactions identified a number of problems, including inadequate documentation. These issues affect not only Prompt Payment Act

[10]Except where otherwise specified within contracts, the act generally provides that agencies pay within 30 days after the designated office receives the vendor invoice or the government accepts the items ordered as satisfactory, whichever is later.

compliance, but the ability to determine whether payments were proper or whether the government received the goods and services paid for under Air Force contracts. We also found that neither DFAS Dayton nor DFAS Denver's Directorate of Finance and Accounting Operations tracks invoices, whether mailed or faxed, from the time they are received until they are entered into the vendor payment system.

For DFAS Dayton, we tested 27 vendor payment disbursement transactions made during fiscal year 1997 as part of our audit of the governmentwide consolidated financial statements.[11] Our tests disclosed that 9 of 27 disbursement transactions were not supported by proper payment documentation, which includes a signed contract, approved voucher, invoice, and receiving report. Of the remaining 18 disbursement transactions, receiving report documentation for 12 transactions did not properly document the date that goods and services were received. Instead, the receiving report documentation showed the date that the document was signed.

At your request, we reviewed 77 vouchers for Bolling AFB contracts paid by DFAS Denver's Directorate of Finance and Accounting Operations in 1997 and 1998 that were obtained by your staff during their review of the DFAS Denver Directorate's vendor payment operations in March 1998. All 77 of the payment vouchers had deficiencies, ranging from incomplete information to identify the individual receiving the goods and services to a missing receiving report. For example, 13 of the 77 DFAS Denver Directorate's payment vouchers were replacement invoices that were marked "duplicate original" or "reprint," possibly indicating that the original invoices had been lost or misdirected before being entered in the vendor payment system. In addition, 31 of the 77 vouchers contained receiving report documentation that omitted the date that goods and services were received.

On March 25, 1998, in response to concerns regarding these 31 vouchers, the DFAS Denver Directorate revised its receiving report requirements to help ensure proper documentation of this date. However, at the end of our review in mid-August 1998, we were told that this problem had not yet been corrected at DFAS Dayton or the other vendor payment operating locations.

[11]Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998).

Our review also showed that 2 of the 77 vouchers had discrepancies similar to those identified as part of the DFAS Dayton investigation. Specifically, one voucher had been voided and resubmitted later without the appropriate interest calculation. The other voucher included an invoice that appeared to have been created by a DFAS Denver Directorate employee because, according to the contract, the contractor lacked invoicing capability. The practice of creating invoices for contractors provides an opportunity for DFAS and Air Force employees to create false invoices. In the absence of computerized invoicing, contractors can submit billing letters that identify quantities, items billed, and costs. Thus, there appears to be no valid reason for DFAS or Air Force employees to create invoices.

In closing, Mr. Chairman, internal control weaknesses that contributed to past fraud in the Air Force's vendor payment process continue. Our report on these issues, released today, details a number of recommendations to help improve the controls over Air Force vendor payments. For example, we recommend that the DFAS Director strengthen payment processing controls by establishing separate organizational responsibility for entering (1) obligations and contract information, (2) invoice and receiving report information, and (3) changes in remittance addresses. We also recommend that the vendor payment system access levels be revised to correspond with the segregation of organizational responsibility and that the number of employees with vendor payment system access be reduced. Until DFAS and the Air Force complete the actions to address control weaknesses in vendor payment systems and processes and maintain accountability over goods and services received, Air Force funds will continue to be vulnerable to fraudulent and improper payments.

Mr. Chairman, this concludes my statement. I will be pleased to answer any questions you or other Members of the Subcommittee may have at this time.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON  RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested