United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate

September 1998

FINANCIAL MANAGEMENT

Improvements Needed in Air Force Vendor Payment Systems and Controls

GAO/AIMD-98-274

GAO

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

Accounting and Information
Management Division

B-280635

September 28, 1998

The Honorable Charles E. Grassley
Chairman, Subcommittee on Administrative Oversight
and the Courts
Committee on the Judiciary
United States Senate

Dear Mr. Chairman:

This report responds to your request that we review two specific cases of fraud involving vendor payments made on behalf of the Air Force. 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.[1] The second case covered fraudulent activities between October 1994 and June 1997 at Castle AFB, California, and the Defense Finance and Accounting Service (DFAS) Dayton resulting in a $435,000 embezzlement and attempted theft of over $500,000. The Dayton case also involved the altering of invoices to improve reported payment performance, thereby depriving government contractors of interest payments.

As agreed with your office, our objectives were (1) to identify internal control weaknesses that contributed to the two fraud cases, (2) to provide our observations on whether the same or similar internal control weaknesses continue to leave Air Force funds vulnerable to fraud or improper payments, and (3) to the extent possible, reconstruct the history of the two contracts associated with the Bolling AFB fraud to determine whether the government received the goods and services paid for under the contracts. We performed our work from October 1997 through August 1998 in accordance with generally accepted government auditing standards. We requested written comments on a draft of this report from the Secretary of Defense or his designee. We had not received comments by the time we finalized our report. Details on our scope and methodology are in appendix I.

Results in Brief

The two cases of fraud resulted from a weak internal control environment. The lack of segregation of duties and other control weaknesses, such as weak controls over remittance addresses, created an environment where

[1]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).

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 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 and 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,[2] which requires that payments made after the due date include interest.

Missing records, another indicator of a weak internal control environment, prevented us from reconstructing the complete history of the two Air Force contracts associated with the Bolling AFB fraud. We also were unable to determine whether the Air Force received the goods and services paid for under these contracts because, in addition to missing records, a number of improper procedures were followed for receipt and control of equipment and services paid for under the contracts. For example, the Air Force employee who was convicted of submitting false claims to the United States directed the contractor to falsify invoices and receiving reports by changing the type and quantity of items received under a delivery order.

Background

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

[2]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.

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.

The Accounting and Auditing Act of 1950 requires agency heads to establish and maintain effective internal controls. Since then, other laws have required renewed focus on internal controls. For example, the Federal Managers' Financial Integrity Act (FMFIA) of 1982 was enacted by the Congress because of repeated reports of fraud, waste, and abuse caused by weak internal controls and control breakdowns. FMFIA requires agency heads to periodically evaluate their systems of internal control using the guidance issued by the Office of Management and Budget (OMB) and to report annually to the President and the Congress on whether their systems conform to internal control standards issued by GAO. Pursuant to FMFIA, OMB Circular A-123, Management Accountability and Control, provides the requirements for assessing controls and GAO's Standards for Internal Control in the Federal Government[3] provide the measure of quality against which controls in operation are assessed. Most recently, the Federal Financial Management Improvement Act of 1996, in focusing on financial management systems, identified internal control as an integral part of those systems.

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.[4] In this regard, we have reported that serious internal control weaknesses have resulted in numerous erroneous and, in some cases, fraudulent payments.[5] For example, $3 million in fraudulent payments were made to a former Navy supply officer on over 100 false invoices.[6]

[3]GAO's Policy and Procedures Manual for Guidance of Federal Agencies, Title 2, Appendix II, Standards for Internal Control in the Federal Government, 1983.

[4]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).

[5]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).

[6]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[7] 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.

During fiscal year 1997, the DFAS Denver Center and its accounting and disbursing offices processed a reported $17.2 billion in vendor payments for the Air Force. The DFAS Denver Center, which was activated in January 1991, is responsible for accounting, disbursing, collecting, and financial reporting for Air Force vendor contracts. As a result of DFAS consolidations between 1991 and 1998, Defense Accounting Offices were closed. Under the DFAS Denver Center, financial services for vendor contracts are now performed by the Directorate of Finance and Accounting Operations, in Denver, Colorado, and five DFAS operating locations at Dayton, Ohio; Limestone, Maine; Omaha, Nebraska; San Antonio, Texas; and San Bernardino, California.

The vendor payment process includes the processing and approval of payments for operational support such as utilities, medical services, and administrative supplies and services. Payments must be supported by (1) a signed contractual document, such as a purchase order, (2) an obligation, (3) an invoice, and (4) a receiving report. If the process is operating as intended, vendor payment team members at the various operating locations are to review these documents for accuracy and completeness and enter information into the vendor payment system—the Integrated Accounts Payable System—to create a payment voucher, which is subsequently approved by a certifying officer. Certifying officers are to compare payment vouchers to invoices and receiving reports to ensure the accuracy of the payment information prior to disbursement. For the first and last payments on a contract, certifying officers are to verify contract information as well. Following certification, the payment information is loaded into the disbursing system—the Integrated Paying and Collecting system.

Before funds are disbursed, an independent check of available obligations (prevalidation) is to be made by electronically comparing vendor payment system transactions to obligations recorded in the General Accounting and Finance System (general ledger). Once available obligations are confirmed, the disbursing system uses the payment transactions generated

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

by the vendor payment system to make the disbursements and report the payment data to the Department of the Treasury. In addition, the vendor payment system generates payment transactions to update the accounting system. Finally, the Merged Accountability and Fund Reporting reconciliations between the accounting, vendor payment, and disbursing systems are performed on a daily basis to help ensure that detail transactions, such as contract expenditures, are in agreement.

Internal Control and System Weaknesses Contributed to Fraud

To reduce the risk of error, waste, or wrongful acts and to reduce the risk of them going undetected, GAO internal control standards require segregation of key duties and responsibilities in authorizing, processing, recording, and reviewing transactions and maintaining custody over assets. No one individual should control all key aspects of a transaction or event without appropriate compensating controls. Also, the individuals performing these duties are to receive qualified and continuous supervision to ensure that the agency's internal control objectives are met. To ensure that financial reports provide timely, accurate information on the results of operations, internal control standards require that transactions and other significant events are to be promptly recorded and properly classified. In addition, periodic evaluations are required to assess risks, identify deficiencies, and effect corrective action.

For the two fraud cases, the primary internal control weakness was the lack of segregation of duties. In each case, the individuals committing the fraud had authority or capability to perform functions that should have been segregated. For example, in the Bolling AFB case, the 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 the Dayton case, the Staff Sergeant, who at different times held positions in accounting and payment processing, was responsible for recording contract data, including obligations; invoice and receiving report information; and remittance addresses. After the Staff Sergeant's access to the Dayton vendor payment system was removed, he was able to perform these functions by obtaining and using the computer password of another employee who had a level of access to the vendor payment system comparable to the level of access the Staff Sergeant previously held.

Internal Control Weaknesses Related to the Bolling AFB Fraud

An Air Force civilian employee, who was the COTR on the two Bolling AFB contracts, had broad authority to request contract amendments, order goods and services, receive and accept the goods and services, and

approve payment for the items received. 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.

In September 1992, the COTR requested that contractor employees submit five false invoices totaling $342,832, for billings of goods and services that had not been ordered or received. According to contractor employees, the COTR told them that he was requesting advance billings to prevent the expiration of unused funding. While DOD has some authority to make advance payments,[8] advance billings are not authorized for this purpose. Contractor employees submitted the five false invoices, as well as false receiving reports for each invoice, as instructed by the COTR.

The COTR also gave the contractor a memo dated October 14, 1992, instructing the contractor to order $500,000 of legislative consulting services from a subcontractor, Applied Quantitative Systems, and include a 25 percent markup ($125,000) for overhead to be retained as the contractor's fee when submitting the invoice to the Air Force. The COTR's memo listed the five false invoices discussed above as partial documentation of these services. However, Applied Quantitative Systems was a fictitious company created by the COTR that had not provided any services under this contract, and the remittance address on the invoice was for a post office box opened by the COTR to receive the $500,000 payment. Had the contractor followed through on the COTR's instructions, it would have eventually billed the government $625,000,[9] sent $500,000 to the COTR's fictitious company address, and kept $125,000 as overhead. However, according to contractor internal review files, management determined that legislative services were outside the scope of the contract and, as a result, did not submit this invoice to the government.

In November 1992, contractor management became aware of the five false invoices that had been submitted at the COTR's request and retrieved from the bank four checks received from the Air Force totaling $322,032 for payment of three[10] of the invoices. The contractor voided the checks and returned them to the Air Force. Reportedly at the request of the

[8]10 U.S.C. 2307.

[9]This amount relates to $342,832 on the five invoices the contractor had already submitted plus an additional $282,168.

[10]One of the three invoices was paid by two checks.

contractor, the COTR had the Air Force withdraw the remaining two invoices totaling $20,800.

Then, in December 1992, the COTR, without the contractor's involvement, prepared 11 false invoices resulting in $504,941 in fraudulent payments. As with the Applied Quantitative Systems invoice, the COTR used his own post office box as the remittance address on the 11 false invoices. The COTR retrieved the payment from the post office box and deposited the funds in two newly established accounts at a bank where he maintained a personal account.

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

Since the 1992-1993 Bolling AFB fraud, contractors are generally required to send invoices to DFAS Denver's Directorate of Finance and Accounting Operations for payment. As a result, COTRs generally do not review or approve invoices. In addition, the Single Agency Manager (SAM) was put in place in March 1995. The mission of SAM, in general, is to provide, manage, operate, and maintain designated information technology services for all applicable components and customers. As a part of that mission, SAM operates and maintains information technology systems. In order to procure information technology systems and services, SAM utilizes contracting offices at the Pentagon and at Bolling AFB. SAM is in the process of implementing a position for contracting officer representatives (COR) who are to be responsible for the direct supervision of COTRs' performance of contract-related duties, such as the writing of technical specifications,

inspection of contractors' technical performance, and submission of receiving reports. A SAM official told us that this change, which is targeted for full implementation by the spring of 1999, is intended to address the lack of close supervision that contributed to the Bolling AFB fraud.

Internal Control Weaknesses Related to Castle AFB and DFAS Dayton Fraud

An Air Force Staff Sergeant was convicted of fraudulent activities at two locations. 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 DFAS Dayton.

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 directed 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 the Merged Accountability and Fund Reporting reconciliation identified a discrepancy between the contract number associated with the invoice in the vendor payment system and the contract number associated with the

invoice 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—in violation of 18 U.S.C. 1001[11]—to avoid interest on late payments and improve reported performance for on-time payments. In July 1998, the Staff Sergeant was sentenced to 12 years imprisonment.

Vendor Payment System Has Serious Control Weaknesses

At DFAS Dayton and DFAS Denver Directorate of Finance and Accounting Operations, we observed internal control weaknesses in the vendor payment process that were similar or the same as those that contributed to the incidents of fraud discussed in this report. In addition, we identified weaknesses in computer security that would permit improper access to the vendor payment system.

Inadequate Access Controls Leave Payment System Vulnerable to Unauthorized Use

The lack of segregation of duties with respect to the level of access to the vendor payment system held by the Staff Sergeant that allowed him to embezzle funds remains widespread. We identified three critical access control weaknesses in the vendor payment system: (1) access levels do not provide adequate functional segregation of duties, (2) the number of staff with such access is excessive and widespread throughout DFAS and the Air Force, and (3) computer security over the operating system and the vendor payment application for DFAS Denver is weak.

With regard to the first issue, an August 1996 Air Force Audit Report[12] 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

[11]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.

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

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. Once these activities are segregated organizationally by assigning them to different individuals, the authority to enter contract data and payment information must be functionally segregated within the vendor payment system application to maintain the integrity of the organizational segregation. Without segregation of these duties and controls over access to the system, appropriate compensating controls need to be in place, such as reviews of remittance address change activity and periodic verification of payment addresses with the vendors.

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 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.

DFAS Denver Center has scheduled operational reviews of all DFAS operating locations for completion by January 1999. These reviews are intended to assess whether DFAS operations comply with DFAS policies and procedures as well as laws and regulations. However, we found that the review program did not address the implementation and effectiveness of internal controls, including the segregation of duties and systems access issues identified in this report. After we briefed the DFAS Denver Center Director about our concerns, he told us that the 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, determined that the Defense Megacenter (DMC) in San Antonio, on which DFAS Denver's Directorate of Finance and Accounting Operations vendor payment system runs, did not appropriately restrict access to powerful system utilities. These utilities enable a user to access and manipulate any data within the mainframe computer and vendor payment system. The DMC had granted this privileged access to an excessive number of users and was not able to provide adequate documentation of management approval and review for most of these 161 users. In addition, the DMC had granted 673 users higher levels of access authority than necessary to perform their duties. These high-level security profiles enable a user to bypass the regular control features, which the mainframe computer and vendor payment system are capable of providing to preclude unintentional or unauthorized manipulation of vendor payment files.

The DISA review also determined that routine system monitoring and oversight was not performed to identify and follow-up on user noncompliance with security standards. This allowed serious security weaknesses to exist, which are commonly exploited by hackers. For example, the review team was able to access user IDs and passwords residing in unsecured files on the system and gain access to other systems. Also, default passwords, which are commonly known, were not disabled. Further, passwords and user IDs were not managed according to DISA policies. In general, all user IDs and passwords were allowed to remain inactive for 90 days, contrary to DISA policy requiring that user IDs and passwords be disabled after 35 days of inactivity. There were also 36 users whose passwords expired after 180 days, and 12 users, including a security administrator, whose passwords were set to never expire, which exceeds the 90-day DISA policy. These situations increase the risk that user IDs will be compromised to gain unauthorized access to DOD systems.

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. Thus, a clerk could obtain the passwords and user IDs of employees with higher access and use this information to enter the vendor payment system and perform all payment processing functions.

DOD does not encrypt passwords and user IDs for unclassified financial data. However, other technological controls could be used to improve user authentication procedures, such as a smart card.[13] Alternatively, other internal controls could be implemented, such as supervisory review and validation of user activity. As with the selection of any internal control, consideration of these alternatives would entail an assessment of the cost and benefits of each.

Inadequate Controls Over Remittance Addresses

The control over remittance addresses remains a weakness. DFAS changed its policy in April 1997 to require that the contractor address listed in the contract be used as the remittance address, but it still permits the use of

[13]Smart cards are access cards containing encoded information and sometimes a microprocessor and a user interface. The encoded information and/or the information generated by the processor are used to gain access to a computer system or facility.

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. In addition, widespread access to the vendor payment system that allows users to enter changes to the remittance address, as discussed earlier, remains a weakness.

The Defense Logistics Agency has an initiative under way intended to validate remittance addresses. Under the Central Contractor Registry,[14] 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 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

Internal controls are put in place not only to help ensure accountability over resources, but also to help an agency achieve full compliance with laws and regulations, such as the Prompt Payment Act of 1982, as amended. This act provides governmentwide guidelines for establishing due dates on commercial invoices and provides for interest payments on invoices paid late. Except where otherwise specified within contracts, the act provides, generally, 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. According to Office of Management and Budget Circular A-125, Prompt Payment, which provides implementation guidance under the act, if the government does

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

not reject items received within 7 days, acceptance will be deemed to occur on the 7th day after receipt. Payments made after the required payment date must include interest. One performance measure used by DFAS to assess operating location performance is the amount of interest paid.

The falsification of payment documentation to improve reported performance for on-time payments was a violation of 18 U.S.C. 1001. In addition, it undermined DFAS Dayton's internal controls over payments and impaired its ability to detect or prevent fraud. According to DFAS internal review and Air Force investigative reports, the Staff Sergeant convicted of embezzlement had also instructed his branch employees to falsify invoice dates in an effort to improve reported payment performance, thereby depriving government contractors of interest on late payments. 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 used faxed invoices to alter invoice receipt dates to avoid late payment interest required by the Prompt Payment Act. According to documents presented at the Staff Sergeant's trial, this was done by using a photocopy of the fax and manually changing the dates and then photocopying the fax again. DFAS Dayton staff then faxed the photocopied document to their own office to create a new date. 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.

In addition, we found that in June 1996, DFAS Dayton implemented an Air Force-wide initiative to improve payment timeliness which generally permitted (1) payment of invoices under $2,500 without receiving reports and (2) acceptance of remittance addresses recorded on invoices without further verification. As of October 1997, the payment of invoices without receiving reports was to be terminated based on legal concerns about compliance with prompt payment and advance payment statutes.

Our review of selected fiscal year 1997 DFAS Dayton and DFAS Denver Directorate of Finance and Accounting Operations vendor payment transactions identified a number of problems, including inadequate

documentation, which affect not only Prompt Payment Act 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. Further, without adequate supporting documentation for disbursements, DFAS cannot ensure that fraud has not occurred.

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.[15] 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.

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

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

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 addition, we reviewed five examples of altered invoices identified by DFAS Dayton staff who had raised concerns about the payment process. We obtained copies of the invoices from the Air Force Audit Agency in June 1998. In one case, the invoice was duplicated and then altered so that interest due the vendor for a late payment was charged to the Defense Stock Fund rather than the appropriate Operation and Maintenance appropriation interest account. DFAS performance measures for late payments do not include interest paid from the Stock Fund. The other four invoices were created to alter the invoice dates by using an invoice template that is a standard file on Air Force and DFAS personal computers. These invoices were substituted for the original invoices submitted by the vendors to avoid interest payments.

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. One means of tracking both mailed and faxed invoices would be for the mail room employees to enter invoice information into the vendor payment system at the time the invoices are received. This control would help ensure that the payment team personnel who are measured on timely performance are not also responsible for establishing the invoice receipt date for one of the key documents that determines when a payment is late.

Documentation Is Not Available to Reconstruct History of Contracts

Due to missing and altered records, we were unable to reconstruct the history of the two contracts associated with the Bolling AFB embezzlement to determine whether the Air Force received the goods and services it paid for under the contracts.

Insufficient Documentation to Reconstruct Contracts

On July 30, 1986, a $49.6 million contract was awarded to provide office automation hardware, software, maintenance, training, and contractor support services for Air Staff offices at the Pentagon and several other locations. Responsibility for managing the contract was assigned to a contracting office at Bolling AFB. The contract ran from July 30, 1986, through December 31, 1991. Under this contract, almost 500 delivery orders were used to acquire goods and services.

Under the Federal Acquisition Regulation (FAR), all records, documents, and other files pertaining to contracts such as this must be maintained for 6 years and 3 months after final payment. According to a Bolling AFB contracting official, the last payment on this contract was made in December 1992. Therefore, records pertaining to this contract should be maintained until at least March 1999. Nevertheless, despite an extensive search of both DFAS and Air Force records, we were unable to locate documentation showing the total amount paid under the contract. Further, neither the Air Force nor DFAS Denver officials were able to locate all the files pertaining to these contracts. As agreed with your office, due to the magnitude of missing records, we did not make further attempts to reconstruct the payment history for the 1986 contract.

A Bolling AFB contracting official told us that a team has been formed to close out the contract. Under the FAR, the team would need to confirm that a final invoice has been approved or a final payment has been made for goods and services received and accepted before closing the contract. The contractor's report on its 1993 internal review of the contract[16] indicated that its records identified approximately $38 million of goods and services that were delivered over a 5-1/2 year period under the 1986 contract. We were unable to locate the contractor records needed to verify this amount. Given the extent of missing records, DFAS and Air Force efforts to confirm that payment was made for goods and services received will be difficult, if not impossible.

On March 13, 1992, a follow-on contract was awarded, effective January 3, 1992, to the company responsible for the first contract. As with the 1986 contract, responsibility for managing this contract was assigned to Bolling AFB and the same COTR. The 1992 contract provided for hardware and software maintenance, technical support, parts, training, and a computer maintenance database. This contract also used delivery orders to acquire

[16]During 1993, the contractor performed an internal review of activities associated with the two Bolling AFB contracts after being contacted by the Secret Service relative to the COTR's improper activities.

goods and services. During the life of the contract, contracting staff awarded 41 delivery orders and 81 modifications to these delivery orders.

Based on available Air Force records, the total amount obligated under the 1992 contract appears to be about $8.2 million. We were able to locate payment vouchers totaling $6.7 million. However, we also found invoices in the contract files totaling over $279,000 for which payment vouchers could not be located. Further, the DFAS Denver Directorate was unable to locate check registers. Thus, we were unable to determine whether these invoices had been paid. As was the case for the 1986 contract, due to poor recordkeeping, neither Bolling AFB nor the contractor were able to accurately determine the status of payments and deliveries under the 1992 contract. The last delivery order for the contract was dated October 1, 1995. However, the contract extended through September 1996. On March 31, 1998, the contractor submitted a final bill totaling $194,000, which listed 16 invoices for which full or partial amounts may still be owed by the Air Force. DFAS officials told us that they did not plan to pay the final bill until they finish reviewing and validating the items included in the invoice because they believe that payment has already been made for some of these items.

Unable to Determine Whether Goods and Services Were Received Due to Inadequate Contract Management

We were also unable to determine whether the Air Force received the goods and services paid for under the two contracts because, in addition to missing records, a number of improper and questionable procedures were followed for receipt and control of equipment and services paid for under the contracts.

As discussed earlier, from June 1988 until February 1993, the COTR had broad authority to order, receive, and accept goods and services. In ordering equipment, the COTR designated the delivery location and later signed for the receipt and acceptance of the equipment. Also, the COTR directed equipment to be delivered to or from an Air Force storage facility. Beginning in 1990, the contractor requested a change in procedures whereby the Air Force would sign for equipment purchased under the 1986 contract but let the contractor store the equipment at the contractor's warehouse until the Air Force was ready to take delivery. However, because neither the Air Force nor the contractor maintained accurate, complete property records on this equipment, we could not determine whether the Air Force received this equipment.

Because of its desirability and portability, computer equipment is highly susceptible to theft. Under DOD's Financial Management Regulation, pilferable items, such as personal computers, are required to be recorded in the property records. We attempted to determine whether the government received 29 computer equipment items identified as being maintained under the contract at Air Force locations in the Washington, D.C., area. We located 10 items and obtained documentation on the disposal of 3 items. Of the 16 remaining items, all of which were computer servers, only 4 were recorded in the property records. However, we were unable to locate the 4 servers. In addition, we could not locate or identify documentation for the 12 remaining servers. Property officials told us that computer equipment delivered and paid for under the contract was not always recorded in property records.

In several instances, the COTR directed the contractor to bill for equipment as maintenance in order to avoid contract limitations on the amount of equipment that could be procured. The contractor's 1993 internal review report stated that equipment was misdescribed as maintenance on 116 of 142 invoices reviewed.

Although the 1992 contract required the contractor to develop a database to track equipment maintenance, neither Air Force nor contractor files contained complete maintenance records for equipment purchased under the contract. According to a contractor official, the contractor's 1993 internal review team inadvertently destroyed the equipment maintenance database that the contractor was required to develop and maintain under the contract. Further, while the 1992 contract required the contractor to provide certificates for completed training, Bolling AFB contract records did not contain training certificates.

Conclusions

Internal control weaknesses that contributed to past fraud in the Air Force's vendor payment process continue. DFAS and the Air Force have not developed adequate segregation of duties to ensure that one individual cannot establish a contract obligation, enter invoice and receiving report information, and change a remittance address. Moreover, the Air Force's vendor payment system is vulnerable to unauthorized users due to weaknesses in operating computer system and local network security. Until DFAS and the Air Force address control weaknesses in systems and processes and maintain accountability over goods and services received, the Air Force vendor payment process will continue to be vulnerable to fraudulent and improper payments.

Recommendations

To address the continuing vulnerabilities in the vendor payment process, 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;
- revise vendor payment system access levels to correspond with the segregation of organizational responsibility delineated above; and
- reduce the number of employees with vendor payment system access by (1) identifying the minimum number of employees needing on-line access to specific functions, (2) determining whether the access levels given to each user are appropriate for the user's assigned duties, and (3) removing access from employees who are no longer assigned to these functions.

To strengthen computer security for the vendor payment system, we recommend that the DISA Director (1) correct the system security control weaknesses in the operating system (mainframe) on which DFAS Denver's vendor payment system application runs and (2) assess the costs and benefits of implementing technological and/or administrative controls over user IDs and passwords.

To ensure that internal controls are properly designed and operating as intended, we recommend that the DFAS Director revise the operational review program to include assessments of the internal controls over the vendor payment process.

To help ensure that vendor payments are proper and that they comply with Prompt Payment Act time frames, we recommend that the DFAS Director ensure that (1) the date that invoices are received and the date that goods and services are received are properly documented and (2) invoices are tracked from receipt through disbursement of funds. In addition, we recommend that the DFAS Director no longer permit the creation of contractor invoices by DFAS employees and require those contractors that lack invoicing capability to submit billing letters.

We are sending copies of this report to the Ranking Minority Member of the Subcommittee on Administrative Oversight and the Courts, Senate Committee on the Judiciary; the Chairmen and Ranking Minority Members of the Senate Committee on Armed Services, the House Committee on National Security, the Senate Committee on Governmental Affairs, the

House Committee on Government Reform and Oversight, and the House and Senate Committees on Appropriations; and the Director of the Office of Management and Budget. We are also sending copies to the Secretary of Defense; the Secretary of the Air Force; the Director, Defense Finance and Accounting Service; the Director, Defense Information Systems Agency; and the Director, Defense Logistics Agency.

Please contact me at (202) 512-9095 if you or your staff have any questions. Major contributors to this report are listed in appendix II.

Sincerely yours,

Lisa G. Jacobson
Director, Defense Audits

Contents

Abbreviations

AFB	air force base
COR	contracting officer representative
COTR	contracting officer's technical representative
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DMC	Defense Megacenter
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FMFIA	Federal Managers' Financial Integrity Act
OMB	Office of Management and Budget
SAM	Single Agency Manager

Objectives, Scope, and Methodology

In accordance with your request, our objectives were to (1) identify internal control weaknesses that contributed to Bolling AFB, Castle AFB, and the DFAS Dayton fraud, (2) provide our observations on whether the same or similar internal control weaknesses at the locations covered by our review continue to leave the Air Force vulnerable to fraud, and (3) to the extent possible, reconstruct the history of the two contracts associated with the Bolling AFB fraud to determine whether the government received the goods and services paid for under the contracts.

To identify internal control weaknesses that contributed to the Bolling AFB and the Castle AFB and DFAS Dayton fraud, we reviewed investigative reports by DFAS internal reviewers and the Air Force's Office of Special Investigations on how these incidents of fraud were accomplished. We also discussed the control weaknesses related to the fraud cases with DFAS Denver and Dayton managers. We compared the activities involved in the fraud with GAO internal control standards and federal agency requirements for assessing controls contained in OMB Circular A-123, Management Accountability and Control. Our work was limited to a review of the fraud incidents and related documentation for which the two individuals were convicted and does not address any ongoing investigations involving any additional participants.

Our observations on the current internal control environment are based on the following.

- A review of the current vendor payment processes at the DFAS Denver Directorate of Finance and Accounting Operations and DFAS Dayton.
- A test of 27 fiscal year 1997 DFAS Dayton vendor payment transactions included in a statistical sample of payment transactions tested as part of our governmentwide consolidated financial statement audit effort.
- A review of 77 vendor payment vouchers processed by DFAS Denver in 1997 and 1998 that were provided to us by Subcommittee staff. We were asked to analyze this sample which was obtained by the Subcommittee staff as part of its review of DFAS Denver vendor payments.
- A review of five examples of altered invoices identified by DFAS Dayton staff, which we obtained from the Air Force Audit Agency.
- A test of computer system access controls for the vendor payment system—Integrated Accounts Payable System and the Central Contractor Registry.
- Discussions with DFAS, Air Force, and Single Agency Manager officials.

To identify significant operating computer system control weaknesses, we reviewed the Defense Information Systems Agency's (DISA) Security Readiness Review methodology and compared it with GAO's Financial Information System and Control Audit Methodology. We also considered the results of Security Readiness Reviews performed by DISA at the Defense Megacenters in San Antonio, Texas, and Warner-Robins AFB, Georgia, which are the data processing centers for DFAS Denver and Dayton, respectively.

In attempting to summarize the history of the 1986 and 1992 Bolling AFB contracts, we

- reviewed Bolling AFB contract files to determine the purpose, scope, and cost of the 1986 Air Staff Office Automation System contract and the 1992 Air Staff CAISS Air Force Follow-on contract and
- reviewed the 1986 and 1992 contract activity using records obtained from Bolling AFB, the Air Force finance office at the Pentagon, and DFAS Denver's Directorate of Finance and Accounting Operations.

In our efforts to determine whether the Air Force received the goods and services paid for under the 1986 and 1992 contracts, we reviewed contract records, payment documents, and systems data at Bolling AFB, the Air Force finance office at the Pentagon, and the Single Agency Manager office at the Pentagon.

We performed our work from October 1997 through August 1998 in accordance with generally accepted government auditing standards. We conducted our review at the 11th Wing Contracting Squadron at Bolling AFB, Washington, DC; the Single Agency Manager office at the Pentagon in Arlington, Virginia; DFAS Dayton in Ohio; the DFAS Denver Center and DFAS Denver Directorate of Finance and Accounting Operations; and the Defense Megacenters at San Antonio, Texas, and Warner-Robbins AFB, Georgia.

We requested comments on a draft of this report from the Secretary of Defense or his designee. We had not received comments by the time we finalized our report.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Gayle L. Fischer, Assistant Director Crawford L. Thompson, Assistant Director, EDP Audits James Ariail, Jr., Senior Auditor Jeffrey Isaacs, Senior Auditor Francine DelVecchio, Communications Analyst
Atlanta Office	Sharon S. Kittrell, Senior EDP Auditor
Dayton Office	Keith McDaniel, Senior Auditor Bill Bricking, Senior Evaluator Roger Corrado, Senior Evaluator
Norfolk Office	Robert Wagner, Project Manager Susan Mason, Evaluator
Office of the General Counsel	Thomas Armstrong, Assistant General Counsel Andrea Levine, Senior Attorney

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

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