United States General Accounting Office

GAO

Report to the Acting Chief Information Officer and the Director of the Austin Automation Center, Department of Veteran Affairs

June 1999

VA INFORMATION SYSTEMS

The Austin Automation Center Has Made Progress in Improving Information System Controls

GAO/AIMD-99-161

GAO
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-282593

June 8, 1999

Mr. Harold F. Gracey, Jr.
Acting Chief Information Officer
Department of Veterans Affairs

Mr. Robert P. Evans
Director, Austin Automation Center
Department of Veterans Affairs

As part of our review of computer security at the Department of Veterans Affairs (VA), we assessed the effectiveness of information system general controls[1] at the Austin Automation Center (AAC). Our review of VA computer security was performed in connection with the department's required annual financial statement audit[2] for fiscal year 1998. Our evaluation included follow-up on the computer security weaknesses we identified at AAC in conjunction with the audit of VA's fiscal year 1997 financial statements.

Today, we are also issuing a report designated for "Limited Official Use," which details the weaknesses we identified at AAC and the current status of corrective actions. This version of the report, which was excerpted for public release, provides a general summary of the weaknesses we identified, the status of corrective actions, and the recommendations we made.

We advised the director of AAC of specific corrective actions that could be taken to address the weaknesses we identified. The results of our evaluation were shared with the VA's Office of Inspector General (IG) for its use in auditing VA's consolidated financial statements for fiscal year 1998.

[1]General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data and programs is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

[2]The Government Management Reform Act of 1994, which expands the Chief Financial Officers Act of 1990, requires that the inspectors general of 24 major federal agencies, including VA, annually audit agencywide financial statements.

Results in Brief

AAC had made substantial progress in correcting specific computer security weaknesses that we identified in our previous evaluation of information system controls. AAC had established a solid foundation for its computer security planning and management program by creating a centralized computer security group, developing a comprehensive security policy, and promoting security awareness. However, AAC had not yet established a framework for continually assessing risks and routinely monitoring and evaluating the effectiveness of information system controls.

We also identified additional computer security weaknesses that increased the risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and destruction of financial and sensitive veteran medical and benefit information on AAC systems. An effective computer security planning and management program would have allowed AAC to identify and correct the types of additional weaknesses that we identified. In addition, AAC continues to run the risk that unauthorized access may not be detected because it had not established a program to identify and investigate unusual or suspicious patterns of successful access to sensitive data and resources. These weaknesses could also affect other agencies that depend on AAC information technology services.

AAC was very responsive to addressing new security exposures identified and corrected several weaknesses before our fieldwork was completed. In commenting on this report, the Acting Assistant Secretary for Information and Technology said VA would implement all of our recommendations by September 30, 1999. Addressing the remaining issues will help ensure that an effective computer security environment is achieved and maintained.

Background

VA is responsible for administering health care and other benefits, such as compensation and pensions, life insurance protection, and home mortgage loan guarantees, that affect the lives of more than 25 million veterans and approximately 44 million members of their families. In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for veterans and their family members.

AAC is one of VA's three centralized data centers. It maintains the department's financial management and other departmentwide systems, including centralized accounting, payroll, vendor payment, debt collection, benefits delivery, and medical systems. AAC also provides, for a fee,

information technology services to other government agencies. As of November 1998, the center either provided or had entered into contracts to provide information technology services, including batch and online processing and workers' compensation and financial management computer applications, for nine other federal agencies.[3]

In fiscal year 1998, the VA's payroll was more than $11 billion and the centralized accounting system processed more than $7 billion in administrative payments. AAC also maintains medical information for both inpatient and outpatient care. For example, AAC systems document admission, diagnosis, surgical procedure, and discharge information for each stay in a VA hospital, nursing home, or domiciliary. In addition, AAC systems contain information concerning each of the guaranteed or insured loans closed by VA since 1944, including about 3.5 million active loans.

As one of VA's three centralized data centers, AAC is part of a vast array of computer systems and telecommunication networks that VA relies on to support its operations and store the sensitive information the department collects in carrying out its mission. The remaining two data centers support VA's compensation, pension, education, and life insurance benefit programs.

In addition to the three centralized data centers, the Veterans Health Administration operates 172 hospitals at locations across the country that operate local financial management and medical support systems on their own computer systems. These data centers and hospitals are interconnected, along with 58 Veterans Benefits Administration regional offices, the VA headquarters office, and customer organizations such as non-VA hospitals and medical universities, through a wide area network. All together, VA's network services over 700 locations nationwide, including Puerto Rico and the Philippines.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of information system general controls over the financial systems maintained and operated by VA at AAC. General controls, however, also affect the security and reliability of nonfinancial information, such as veteran medical and loan data, maintained at this processing center.

[3]At the time of our review, GAO had contracted with AAC for information technology services.

Specifically, we evaluated information system general controls intended to

- protect data, files, programs, and equipment from unauthorized access, modification, and destruction;
- prevent the introduction of unauthorized changes to application and system software;
- provide adequate segregation of duties involving application programming, system programming, computer operations, security, and quality assurance;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an effective computer security planning and management program is in place.

We restricted our evaluation to AAC because VA's Office of Inspector General was planning to review information system general controls for fiscal year 1998 at the Hines and Philadelphia benefits delivery centers.

To evaluate information system general controls, we identified and reviewed AAC's general control policies and procedures. We also tested and observed the operation of information system general controls over AAC's information systems to determine whether they were in place, adequately designed, and operating effectively. In addition, we determined the status of previously identified computer security weaknesses, but did not perform any follow-up penetration testing.

We performed our review from October 1998 through March 1999, in accordance with generally accepted government auditing standards. Our evaluation was based on the guidance provided in our Federal Information System Controls Audit Manual (FISCAM)[4] and the results of our May 1998 study of security management best practices at leading organizations.[5]

After we completed our fieldwork, the director of AAC provided us with updated information regarding corrective actions. We did not verify these corrective actions but plan to do so as part of future reviews.

[4]Federal Information System Controls Audit Manual, Volume I – Financial Statement Audits (GAO/AIMD-12.19.6, January 1999).

[5]Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

VA provided us with written comments on a draft of this report, which are discussed in the "Agency Comments" section and reprinted in appendix I.

AAC Has Acted to Improve Security

AAC has made substantial progress in addressing the computer security issues we previously identified. At the time of our review in 1998, AAC had corrected 40 of the 46 weaknesses that we discussed with the director of AAC and summarized in our September 1998 report on VA computer security.[6] AAC had addressed most of the access control, system software, segregation of duties, and service continuity weaknesses we identified in 1997 and had improved computer security planning and management. For example, AAC had

- reduced the number of users with access to the computer room,
- restricted access to certain sensitive libraries, audit information, and utilities,
- established password and dial-in access controls,
- developed a formal system software change control process,
- expanded tests of its disaster recovery plan, and
- established a centralized computer security group.

AAC was also proactive in addressing additional computer security issues we identified during our current review.

Key Issues Were Still Outstanding

We identified a continuing risk of unauthorized access to financial and sensitive veteran medical and benefit information because the center had not fully implemented a comprehensive computer security planning and management program. If properly designed, such a program should identify and correct the types of additional access control and system software weaknesses that we found. In addition, AAC risks certain types of unauthorized access not being detected because it had not completely corrected the user access monitoring weaknesses we previously identified.

[6] Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175, September 1998).

Computer Security Planning and Management Is Essential

Our May 1998 study of security management best practices found that a comprehensive computer security planning and management program is essential to ensure that information system controls work effectively on a continuing basis. Under an effective computer security planning and management program, staff (1) periodically assess risks, (2) implement comprehensive policies and procedures, (3) promote security awareness, and (4) monitor and evaluate the effectiveness of the computer security environment. In addition, a central security staff is important for providing guidance and oversight for the computer security planning and management program to ensure an effective information system control environment.

AAC had established a solid foundation for its computer security planning and management program by creating a centralized computer security group, developing a comprehensive security policy, and promoting security awareness. However, AAC had not yet instituted a framework for continually assessing risks or routinely monitoring and evaluating the effectiveness of information system controls. In March 1999, the director of AAC told us that the center plans to expand its computer security planning and management program to include these aspects. In addition, the director told us that AAC had augmented its security management organization by hiring two additional security experts in May 1999. A comprehensive computer security planning and management program should provide AAC with a solid foundation for ensuring that appropriate controls are designed, implemented, and operating effectively.

Risk Assessments Were Not Performed When Significant Changes Occurred

Periodically assessing risk is an important element of computer security planning because it provides the foundation for the other aspects of computer security management. Risk assessments not only help management determine which controls will most effectively mitigate risks, but also increase awareness and, thus, generate support for adopted policies and controls. An effective risk assessment framework generally includes procedures that link security to business needs and provide for continually managing risk.

VA policy requires that risk assessments be performed when significant changes are made to a facility or its computer systems, but at least every 3 years. AAC had not formally reassessed risk since 1996 even though significant changes to the facility and its systems had occurred. For example, AAC management told us that the center had replaced its mainframe computer, implemented a new mainframe operating system,

and expanded the facility to accommodate a VA finance center in 1998. Although the director of AAC told us in March 1999 that changes in computer security risks were considered by implementation teams responsible for these events, documentation of such considerations were not available. Formal risk assessments should be performed for such significant changes. The director of AAC also told us that management would perform a risk assessment later in 1999 to comply with VA policy.

One reason that AAC had not formally assessed risks when these significant changes occurred was that the center had not developed a framework for assessing and managing risk on a continuing basis. In March 1999, the director of AAC told us that a risk assessment framework would be developed and added to the AAC security handbook. According to the director, this planned risk assessment framework will

- define the types of changes that require a risk assessment;
- specify risk assessment procedures that can be adapted to different organizational units;
- indicate who should conduct the assessment, preferably a mix of individuals with knowledge of business operations, security controls, and technical aspects of the computer systems involved; and
- describe requirements for documenting the results of the assessment.

Information System Controls Were Not Routinely Evaluated

In addition to assessing risk to identify appropriate controls, it is also important to determine if the controls in place are operating as intended to reduce risk. Our May 1998 study of security management best practices found that an effective control evaluation program includes processes for (1) monitoring compliance with established information system control policies and guidelines, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities. AAC had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Such a program would allow AAC to ensure that policies remain appropriate and that controls accomplish their intended purpose.

Although AAC had substantially corrected previously identified computer security weaknesses, we tested additional access and system software controls and found weaknesses that posed risks of unauthorized modification, disclosure, or destruction of financial and sensitive veteran medical and benefit information. These weaknesses included inadequately limiting access of authorized users to sensitive data and programs, maintaining the system software environment, and reviewing network

security. Several of these weaknesses could have been identified and corrected if AAC had been monitoring compliance with established procedures. For example, periodically reviewing AAC user access authority to ensure that it was limited to the minimum required access level based on job requirements would have allowed AAC to discover and fix the types of additional access control weaknesses we identified. Likewise, routinely evaluating the technical implementation of its system software would have permitted AAC to eliminate or mitigate the additional system software exposures we identified.

A program to regularly test information system controls would also have allowed AAC to detect additional network security weaknesses. For example, using network analysis software designed to detect network vulnerabilities, we determined that intrusion attempts on 2 of the 10 network access control paths would not be detected. Although AAC fixed this problem before our fieldwork was completed, AAC staff could have identified and corrected this exposure using similar network analysis software available to them. AAC staff told us that they also plan to begin evaluating the intrusion detection system periodically.

In addition, AAC had not established a process to test network security when major changes to the network occur. Although AAC had used network analysis software to detect network vulnerabilities earlier in October 1998, we determined that both a production and a development network system had a system program with vulnerabilities commonly known to the hacker community. These vulnerabilities could have provided the opportunity to bypass security controls and gain unlimited access to AAC network systems. Although AAC staff determined that the vulnerable programs were no longer needed and deleted them before our fieldwork was completed, these vulnerabilities could have been prevented had network security been reassessed when the network environment changed.

Certain User Access Activities Were Not Adequately Monitored

AAC was also not adequately monitoring certain user access activity. A comprehensive user access monitoring program would include routinely reviewing user access activity to identify and investigate both failed attempts to access sensitive data and resources and unusual or suspicious patterns of successful access to sensitive data and resources. Such a program is critical to ensuring that improper access to sensitive information would be detected.

Because the volume of security information available is likely to be too voluminous to review routinely, the most effective monitoring efforts are those that selectively target unauthorized, unusual, and suspicious patterns of access to sensitive data and resources, such as security software, system software, application programs, and production data. AAC had begun reviewing failed attempts to access sensitive data and resources, but had not established a program to monitor successful access to these resources for unusual or suspicious activity. In March 1999, the director of AAC told us that the center is expanding its user access activity monitoring to identify and investigate unusual or suspicious patterns of access to sensitive resources, such as

- updates to security files that were not made by security staff,
- changes to sensitive system files that were not performed by system programmers,
- modifications to production application programs that were not initiated by production control staff,
- revisions to production data that were completed by system or application programmers, or
- deviations from normal patterns of access to sensitive veteran medical and benefit data.

Additional Computer Security Weaknesses Were Identified

In addition to the access activity monitoring and computer security program planning and management weaknesses that remain open from 1997, we identified 16 additional issues during our 1998 review. For example, AAC had not

- restricted access to certain sensitive data and programs based on job responsibilities,
- routinely reviewed access authorities granted to employees to ensure that they were still appropriate,
- adequately reviewed certain components of its operating system to ensure continued system integrity,
- adequately documented changes to network servers,
- documented testing of certain emergency changes to its financial management systems, or
- issued technical security standards for maintaining the integrity of system and security software for certain operating system environments.

AAC had corrected 6 of the 16 additional issues identified in 1998 before we completed our site visit in Austin. Addressing the remaining additional issues should help AAC ensure that an effective computer security environment is achieved and maintained. We discussed these issues with AAC management and staff and were told that they would be addressed by September 1999.

Conclusions

AAC had made substantial progress in improving information system general controls. In addition to correcting most of the access control, system software, segregation of duties, and service continuity weaknesses we had previously identified, AAC had strengthened its computer security planning and management program by creating a centralized computer security group, developing a comprehensive security policy, and promoting security awareness. Until AAC completes implementing its computer security planning and management program by establishing a framework for continually assessing risks and routinely monitoring and evaluating the effectiveness of information system controls, it will not have adequate assurance that appropriate controls are established and operating effectively.

We identified additional access, system software, and application change control weaknesses that continued to place financial and sensitive veteran medical and benefit information on AAC systems at risk of improper modification, disclosure, or destruction and assets at risk of loss. Unauthorized access may not be detected because AAC had not begun identifying and investigating unusual or suspicious patterns of successful access to sensitive data and resources. AAC could have identified and corrected these types of weaknesses, which could also adversely affect other agencies that depend on AAC for computer processing support, had it fully implemented an effective computer security planning and management program.

Recommendations

We recommend that the Acting VA Chief Information Officer (CIO) work with the director of AAC to

- implement policies and procedures for assessing and managing risk on a continuing basis;
- establish processes for (1) monitoring compliance with established information system control policies and procedures, (2) testing the

effectiveness of information system controls, and (3) improving information system controls based on the results of these activities; and
- expand the center's user access activity monitoring program to identify and investigate unusual or suspicious patterns of successful access to sensitive data and resources for unauthorized access.

We also recommend that the Acting VA CIO coordinate with the director of AAC to ensure that the remaining computer security weaknesses are corrected. These weaknesses are summarized in this report and detailed in a separate report, which is designated for "Limited Official Use," also issued today.

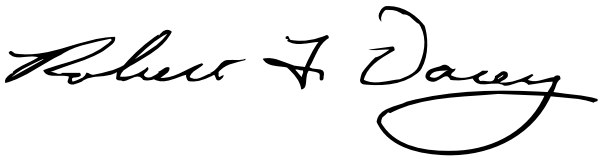
Agency Comments

In commenting on a draft of this report, VA agreed to implement our recommendations by September 30, 1999. Specifically, VA stated that AAC would update its security handbook to include a risk assessment framework, establish a program to routinely monitor and evaluate the effectiveness of controls, and complete procedures for monitoring successful access to sensitive computer resources by the end of September 1999. VA also informed us that AAC had taken action to correct all but three of the other weaknesses we identified and plans to address the remaining weaknesses by September 30, 1999.

Within 60 days of the date of this letter, we would appreciate receiving a statement on actions taken to address our recommendations.

We would like to thank AAC for the courtesy and cooperation extended to our audit team. We are sending copies of this report to Senator Arlen Specter, Senator Ted Stevens, Senator Robert C. Byrd, Senator Fred Thompson, Senator Joseph Lieberman, Senator John D. Rockefeller IV, Representative C. W. Bill Young, Representative Lane Evans, III, Representative Bob Stump, Representative David Obey, Representative Dan Burton, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of Senate and House Committees. We are also sending copies to Togo D. West, Jr., Secretary of Veterans Affairs and the Honorable Jacob J. Lew, Director of the Office of Management and Budget. In addition, copies will be made available to others upon request.

If you have any questions or wish to discuss this report, please contact me at (202) 512-3317. Major contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Consolidated Audit and
Computer Security Issues

Contents

Abbreviations

AAC	Austin Automation Center
CIO	chief information officer
FISCAM	Federal Information System Controls Audit Manual
IG	inspector general
VA	Department of Veterans Affairs

Comments From the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY
WASHINGTON DC 20420

APR 13 1999

Mr. Gene L. Dodaro
Assistant Comptroller General
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro,

The Austin Automation Center (AAC) Director and I appreciate the opportunity to comment on the GAO report entitled, "VA Information Systems – The AAC Has Made Progress in Improving Information Systems Controls," that was provided to both the AAC and to my office. I am satisfied with the improvements the AAC has made to date to address the findings by the General Accounting Office in the 1997 audit and your reevaluation in 1998/1999. The AAC's enhanced general security management and planning program is still evolving and is nearing completion.

During the course of the audit, the GAO team members and the AAC technical staff and Director discussed the AAC plans that are underway to complete all outstanding activities. The remaining items have subsequently either been completed or will be later this year. As a result, most necessary actions identified in your draft report have been completed. With the exception of the items referenced below, all items have been completed. Specifically:

- The AAC will have the standard employee profiles based on job responsibilities completed by September 30, 1999.
- The AAC will complete the procedures for monitoring successful access to other sensitive computer resources by September 30, 1999.
- The AAC will conduct an unannounced disaster recovery plan test by September 30, 1999.
- The AAC will complete the technical security standards for operating system environments other than the mainframe environment (which was already complete) by June 30, 1999.
- The AAC will perform a risk assessment and update the AAC Security Handbook to include a risk assessment framework by September 30, 1999.

Page 2.

Mr. Gene Dodaro

- The AAC will establish a program to monitor and evaluate the effectiveness of information system controls on a routine basis by September 30, 1999.

The AAC Director and staff take pride in all the accomplishments they have made to enhance and improve the AAC computer security environment. The AAC Director and I invite you to revisit the AAC in November 2000 to reevaluate the security posture of the AAC. Again, I appreciate GAO's assistance in this review. I am especially appreciative of the professional working relationship you and your team members have established with the AAC Director and the AAC technical staff. If you have any questions concerning this, please call me at 202-273-8842 or contact Bob Evans, AAC Director, at 512-326-6000.

Sincerely,

Harold F. Gracey, Jr.
Acting Assistant Secretary for
Information and Technology

Major Contributors to This Report

Accounting and Information Management Division

Lon C. Chin, Assistant Director
Vernon Conyers, Jr., Assistant Director
Edward M. Glagola, Jr., Assistant Director
Suzanne Lightman, Auditor
Walter P. Opaska, Senior EDP Auditor
Christopher J. Warweg, Senior EDP Auditor

Dallas Field Office

David W. Irvin, Assistant Director
Debra M. Conner, Senior EDP Auditor
Shannon Q. Cross, Senior Evaluator
Charles M. Vrabel, Senior EDP Auditor

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00