United States General Accounting Office

GAO

Report to the Secretary of Veterans Affairs

October 1999

INFORMATION SYSTEMS

The Status of Computer Security at the Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

GAO/AIMD-00-5

GAO
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-283225

October 4, 1999

The Honorable Togo D. West, Jr.
The Secretary of Veterans Affairs

Dear Mr. Secretary:

We reviewed information system general controls[1] at the Department of Veterans Affairs (VA) in connection with VA's required annual consolidated financial statement audit[2] for fiscal year 1998. Our evaluation included follow-up on departmentwide computer security planning and management weaknesses and specific computer security weaknesses we identified at the Austin Automation Center (AAC) in conjunction with the audit of VA's fiscal year 1997 financial statements.[3] On June 8, 1999, we issued a separate report to the acting VA Chief Information Officer (CIO) and the director of AAC that details the results of our review at AAC.[4] We also reviewed VA Office of Inspector General (OIG) and consultant reports regarding computer security at Veterans Benefits Administration (VBA) and Veterans Health Administration (VHA) facilities. These site reports included recommendations to correct the security weaknesses identified. The results of our underlying reviews were shared with VA's Office of Inspector General (OIG) 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.

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

[4]*VA Information Systems: The Austin Automation Center Has Made Progress In Improving General Computer Controls* (GAO/AIMD-99-161, June 1999).

The purpose of this report is to advise you of the status of computer security throughout VA.

Results in Brief

In September 1998, we reported that VA's information system controls placed critical department operations, such as financial management, health care delivery, benefit payments, and other operations, at risk of misuse and disruption. Since then, VA organizations have taken actions to correct some of the weaknesses we reported and independently initiated actions to improve certain aspects of their computer security management programs. However, progress in correcting the weaknesses we identified in our September 1998 report has been inconsistent across VA organizations, and efforts to improve local computer security management programs were not part of a coordinated, departmentwide effort.

In connection with VA's fiscal year 1998 consolidated financial statement audit, we and VA's OIG continued to find serious problems related to the department's control and oversight of access to its information systems. These weaknesses placed sensitive information, including financial data and sensitive veteran medical and benefit information at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. VA has recognized the significance of these problems and reported information system security as a material weakness in its Federal Managers' Financial Integrity Act (FMFIA) report for 1998.

In September 1998, we also reported that the primary reason for VA's continuing information system control problems was that the department did not have a comprehensive computer security planning and management program. To strengthen its departmentwide computer security management program, VA established a centrally managed security group in February 1999 and an Information Security Working Group, which includes representatives from the central security group and all VA line and staff organization security groups, in March 1999. The Information Security Working Group developed a departmentwide plan to improve information system security throughout VA and establish a departmentwide computer security planning and management program. This plan includes initiatives that would generally address the key elements of a comprehensive security planning and management program. Because this multi-year plan, which is scheduled to be fully implemented by January 2003, is at an early stage of development, its ultimate effectiveness cannot yet be assessed. VA's success in improving information security is largely

dependent on the level of commitment to this throughout VA and adequate resources being effectively dedicated to implement its departmentwide plan.

As VA implements its computer security management program, establishing detailed guidance can help ensure that requirements of this program are implemented fully and consistently throughout the department. This guidance should include developing a framework for conducting risk assessments; monitoring system and user access; and monitoring compliance with established procedures and testing control effectiveness.

In commenting on a draft of this report, VA concurred with all our recommendations. VA stated that the CIO will report progress in implementing the computer security management program as well as progress correcting specific weaknesses. Also, VA stated that the CIO will develop the detailed processes described above as part of a departmentwide security policy framework.

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. VA operates the largest healthcare delivery system in the United States and reported spending more than $17 billion on medical care in fiscal year 1998. The department also processed more than 42 million benefit payments totaling about $22 billion in fiscal year 1998 and provided life insurance protection through more than 2.4 million policies that represented about $23 billion in coverage at the end of fiscal year 1998.

In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for veterans and their family members. The VA maintains medical information for both inpatient and outpatient care. For example, the department records admission, diagnosis, surgical procedure, and discharge information for each stay in a VA hospital, nursing home, or domiciliary. The VA also stores information concerning health care provided to and compensation received by ex-prisoners of war. In addition, the VA maintains information concerning each of the guaranteed or insured loans closed by VA since 1944, including about 3.5 million active loans.

The VA relies on a vast array of computer systems and telecommunication networks to support its operations and store the sensitive information the department collects in carrying out its mission. Three centralized data centers–located in Austin, Texas; Hines, Illinois; and Philadelphia, Pennsylvania–maintain the department's financial management systems; process compensation, pension, and other veteran benefit payments; and manage the veteran life insurance programs.

AAC maintains VA's departmentwide systems, including centralized accounting, payroll, vendor payment, debt collection, benefits delivery, and medical systems. In fiscal year 1998, the VA's payroll was over $11 billion and the centralized accounting system generated over $7 billion in administrative payments. The center also provides information technology services, for a fee, to other government agencies, including GAO.

The other two centralized data centers support VA's Veterans Benefits Administration (VBA) programs. The Hines Benefits Delivery Center (BDC) processes information from VA systems that support the compensation, pension, and education applications for VBA's 58 regional offices. The Philadelphia BDC is primarily responsible for supporting VA's life insurance program.

In addition, the Veterans Health Administration (VHA) operates 172 hospitals at locations across the country that process local financial management and medical support systems on their own computer systems. The medical support systems manage information on veteran inpatient and outpatient care, as well as admission and discharge information, while the main medical financial system–the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) system–controls most of the $17 billion in funds that VA reported spending on medical care in fiscal year 1998. The IFCAP system also transmits financial and inventory information daily to the Financial Management System in Austin.

The three VA data centers, as well as the 172 VHA hospitals, 58 VBA regional offices, the VA headquarters office, and customer organizations such as non-VA hospitals and medical universities, are all interconnected through a wide area network. Altogether, VA's network services over 700 locations nationwide, including Puerto Rico and the Philippines.

Objectives, Scope, and Methodology

Our objectives were to determine the status of computer security at VA and evaluate computer security planning and management throughout the department. To determine the status of computer security, we assessed VA's efforts to correct computer security weaknesses discussed in our September 1998 report;[5] evaluated information system general controls at AAC; and reviewed VA's fiscal year 1998 financial statement audit report, VA's 1998 FMFIA report, and VA OIG and consultant reports regarding computer security at VBA and VHA facilities.

We restricted our review of information system general controls to AAC because the VA's OIG planned to evaluate these controls at VBA and VHA facilities as part of the department's fiscal year 1998 financial statement audit. As part of this work, the VA OIG tested selected security planning and management, access, segregation of duties, and service continuity controls at the Philadelphia BDC; followed up on certain previously reported weaknesses at the Hines BDC; and performed limited tests of security planning and management, access, system software, application development, segregation of duties, and service continuity controls at a medical facility, the Carl T. Hayden Medical Center. We reviewed the OIG's information system general control work at these facilities and the resulting reports. In July 1999, VBA provided us with information regarding actions to correct security weaknesses reported by the OIG. However, the operating effectiveness of these actions still needs to be verified.

To evaluate information system general controls at AAC, we identified and reviewed general control policies and procedures. We also tested and observed the operation of information system general controls at AAC to determine whether these controls were in place, adequately designed, and operating effectively. Our evaluation was based on our *Federal Information System Controls Audit Manual* (FISCAM),[6] which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data associated with federal agency operations. In addition, we determined the status of previously identified AAC computer security weaknesses, but did not perform any follow-up penetration testing. We requested and received

[5] *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 23, 1998).

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

comments on the results of our evaluation from the acting VA CIO and the director of AAC. We did not verify VA statements regarding corrective actions taken subsequent to our AAC site visit, but plan to do so during future reviews.

To evaluate computer security planning and management practices throughout VA, we held discussions with headquarters, VBA, and VHA officials. We also reviewed current computer security policies and procedures as well as VA's plan to improve information security and establish a departmentwide computer security planning and management program. Our evaluation was based on the results of our May 1998 study of security management best practices at leading organizations,[7] which identifies key elements of an effective information security program. This guide, which incorporates many of the concepts in the National Institute of Standards and Technology's September 1996 publication, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, and in the Office of Management and Budget's February 1996 revision of Circular A-130, Appendix III, "Security of Federal Automated Information Resources", has been endorsed by the federal government's CIO Council.

We performed our work at VA headquarters, VBA, VHA, and AAC from October 1998 through July 1999, in accordance with generally accepted government auditing standards.

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.

Actions to Improve Computer Security Were Inconsistent Across VA

In September 1998, we reported that VA's information system controls placed critical department operations, such as financial management, health care delivery, benefit payments, and other operations at risk of misuse and disruption. Since then, VA organizations have taken some actions to correct the computer security weaknesses we reported, with some organizations making more progress than others. Although progress in correcting weaknesses was uneven across VA organizations, each organization had initiated actions to improve certain aspects of their computer security planning and management programs. However, these

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

efforts were performed independently and not coordinated under a departmentwide computer security planning and management program.

VA Organizations Addressed Previously Reported Weaknesses to Varying Degrees

Actions taken to correct the weaknesses we reported in September 1998 were uneven across VA organizations. AAC had corrected most of the specific computer security issues we reported in September 1998. As part of this effort, the center had reduced the number of users with access to the computer room; restricted access to certain sensitive libraries, audit information, and utilities; improved ID and password management controls; developed a formal system software change control process; and expanded tests of its disaster recovery plan.

In contrast, the VBA benefits delivery centers were still in the process of correcting most of the weaknesses we reported in September 1998. A VBA task force, which was established to review the administration's information security posture and develop recommendations for correcting computer security weaknesses, had prepared a number of recommendations to correct policy shortcomings and access control concerns identified at the Hines and Philadelphia benefits delivery centers. In addition, VBA management told us that the benefits delivery centers had initiated corrective actions for all of the weaknesses we reported. However, information system controls reviews performed by VA's OIG as part of VA's fiscal year 1998 financial statement audit found that only one of the seven weaknesses we reported had been fully corrected at the Philadelphia BDC. Similarly, VA OIG information system controls work showed that corrective actions for at least five of the seven weaknesses we reported at the Hines BDC had not been completed. For example, VA's OIG found that the Philadelphia BDC had limited the number of invalid password attempts allowed for the master security administration ID, but still needed to begin reviewing user access authority to ensure that access privileges are appropriate. VA's OIG also reported that neither the Hines nor Philadelphia benefits delivery centers had established a program to routinely monitor network or mainframe user access activity.

In August 1999, VBA management told us that both the Hines and Philadelphia benefits delivery centers had begun monitoring user access activity. VBA management also told us that the Philadelphia BDC had begun periodically reviewing user access authorities.

Furthermore, the status of most of the weaknesses we reported at the Albuquerque and Dallas medical centers in September 1998 was not evident because VA and VHA reports on follow-up actions did not specifically address the weaknesses that we previously reported. In addition, neither the VA nor VHA central security groups had verified that reported corrective actions, such as control mechanisms and/or policy adjustments, were operating as intended. In responding to VHA follow-up efforts, the Albuquerque medical center indicated that it had not yet implemented a targeted monitoring program for its telecommunications system. However, the status of the other access control, ID and password management, service continuity, and security management weaknesses we reported at the Albuquerque and Dallas medical centers in September 1998 was not specifically addressed. In July 1999, the director of VHA's Medical Information Security Service (MISS)[8] told us that he will follow up on the specific weaknesses we reported at the Albuquerque and Dallas medical centers in September 1998 and verify that reported corrective actions are operating effectively.

Actions to Improve Computer Security Management Were Not Coordinated

In addition to efforts to correct specific weaknesses, VA organizations have taken some other actions to improve computer security planning and management since our previous review. However, none of the organizations we visited had implemented a comprehensive computer security planning and management program. In addition, efforts to improve computer security management were initiated independently and not coordinated as part of a departmentwide program. Until these efforts are coordinated centrally, VA will have little assurance that individual computer security planning and management programs are consistent with departmentwide requirements and priorities.

Since September 1998, AAC, VBA, and VHA had all acted to improve computer security planning and management.

- AAC had established a centralized computer security group, developed a comprehensive security policy that covered all aspects of the center's interconnected environment, and established technical security standards to implement this policy for one of its operating environments. In May 1999, the director of AAC told us that the center

[8]MISS is the organization in VHA's Office of the CIO that manages the national VHA information security program.

also plans to develop a risk assessment framework, a program to monitor and evaluate the effectiveness of information system controls, and technical security standards for its other operating environments by the end of September 1999.

- VBA had established a centralized computer security group and implemented a self-assessment tool to assist VBA facilities in generating information system security plans that satisfy OMB Circular A-130.[9] In July 1999, VBA's Acting Information Security Officer told us that the administration was updating its security policies and procedures. VBA management also told us that a risk assessment, along with a plan to mitigate the vulnerabilities identified, had been completed for the Hines BDC and that VBA planned to perform a risk assessment at the Philadelphia BDC by the end of September 1999. In addition, the Acting Information Security Officer told us that VBA plans to establish a program in fiscal year 2000 for routinely assessing risk and testing the effectiveness of established information system general controls at VBA facilities.
- VHA's central security group, MISS, had distributed a risk assessment tool to VHA facilities. MISS had also expanded the information system control checklists that (1) are provided to VHA facilities as security self-assessment tools and (2) guide MISS's triennial security reviews at VHA facilities. In July 1999, the director of MISS told us that VHA was also updating its security policies to develop a more concise overall policy along with an accompanying handbook that provides additional guidance for implementing the policy. MISS staff also told us in July 1999 that it plans to hire a consultant to follow up on a VHA network risk assessment and penetration study performed in 1998. VHA plans to expand this assessment, which it anticipates performing annually, to include intranet activity and internet web sites. VHA also plans to contract with consultants to (1) develop procedures for certifying and accrediting VHA systems and applications and (2) obtain additional technical expertise to assist MISS in performing the more technical aspects of the triennial site visits and develop detailed procedures and guidance that will allow MISS to perform these steps in the future.

[9]OMB Circular A-130, Appendix III, establishes a minimum set of controls for agencies' automated information security programs, including assigning responsibility for security, security planning, periodic review of security controls, and management authorization of systems to process information.

In our May 1998 study of information security best practices, we reported that central coordination is important when managing information security risks in highly interconnected environments, such as VA's. In addition, this study found that central security groups that coordinate and oversee an organization's computer security program were able to achieve some efficiencies and increase consistency in implementing security programs. However, actions taken by AAC, VBA, and VHA to improve computer security planning and management were not coordinated. Consequently, different organizations had sometimes developed or begun developing similar aspects of computer security planning and management in isolation. For example, both AAC and VBA had begun developing separate programs for assessing risk and testing the effectiveness of information system controls at their facilities. In addition, VBA and VHA had developed different types of security self-assessment tools for organizational units. Further, AAC had developed technical security standards for its primary computing environment and was developing standards for additional computing environments that could be useful to other organizations.

Sensitive Data and Programs Were Still Vulnerable to Unauthorized Access

Despite efforts to improve computer security, financial and sensitive veteran medical and benefit information on VA systems continued to be vulnerable to unauthorized access. In connection with the VA's fiscal year 1998 consolidated financial statement audit, we and the VA OIG continued to find serious problems related to the department's control and oversight of access to its systems. VA still had not adequately limited the access granted to authorized users, appropriately segregated incompatible duties among computer personnel, properly managed user IDs and passwords, or routinely monitored access activity. As a result, VA's computer systems, programs, and data were still at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction occurring without detection. VA recognized the seriousness of these problems and began reporting information system security as a material FMFIA weakness in 1998.

Subsequent to our fieldwork, VA provided us with updated information regarding corrective actions to address the security weaknesses we identified at AAC. In July 1999, VBA also provided us with information regarding actions to correct security weaknesses reported by VA's OIG. However, these reported actions, which are noted below, will need to be verified to ensure that they are operating effectively.

Access Authority Was Not Appropriately Limited for Authorized Users

A key weakness in VA's internal controls was that the department had not sufficiently restricted access for authorized users. Organizations can protect information from unauthorized changes or disclosures by granting employees authority to read or modify only those programs and data that are necessary to perform their duties and periodically reviewing access granted to ensure that it is appropriate. VA, however, had not adequately limited access to financial and sensitive veteran medical and benefit information maintained on its systems.

We and VA's OIG found instances where AAC, VBA and VHA facilities had not sufficiently restricted access to sensitive data and programs based on job responsibility.

- At AAC, access to certain sensitive data and programs was not restricted based on job responsibility. This access increased the risk that users could circumvent security controls, improperly modify financial data, or disclose sensitive veteran medical and benefit information maintained at AAC. AAC limited access to most of the data and programs that we identified before we completed our fieldwork. In March 1999, the director of AAC told us that access to the remaining data had been appropriately restricted.
- At the Philadelphia Insurance Center, 265 users, including computer specialists, secretaries, and students, who were not authorized to perform data entry functions in the Awards Data Entry (ADE) system, which is used to initiate insurance awards, had the ability to read, write and delete this information through the operating system software. One hundred and thirty-two insurance program staff members were also provided access to ADE information that exceeded their authorization through the operating system software. This unnecessary access could lead to improper insurance payments. In July 1999, VBA management told us that unauthorized access to ADE data that was allowed through the operating system software had been eliminated.
- At the Carl T. Hayden medical facility, 17 of 18 users with access to the operating system software had unnecessary privileges that provided the opportunity to bypass security controls. As a result, sensitive veteran medical information stored at this facility is vulnerable to improper disclosure.

One reason that these problems existed was because user access authority was not being reviewed periodically. Such periodic reviews could have allowed VA to identify and correct inappropriate access.

VA's OIG also continued to find instances where VBA and VHA facilities were not promptly removing unused or unneeded IDs. Although the Philadelphia BDC had begun to review inactive accounts established for users at remote locations, these reviews were not always effective. For example, a BDC review for one regional office identified 87 users who had never logged on and 6 users who had not logged on since 1996. However, the regional office directed the Philadelphia BDC to delete only one user account. Despite efforts to identify and remove inactive accounts, VA's OIG also found that 231 users at the Carl T. Hayden medical facility had never signed on to the system. Not promptly removing unused and unnecessary IDs increases the risk that these IDs could be used to gain unauthorized access to VA computer systems.

In August 1999, VBA management told us that VBA is in the process of matching system users to personnel files to remove user IDs for terminated employees from the Hines and Philadelphia benefits delivery centers.

Computer Duties Were Not Properly Segregated

In addition to limiting user access authority, the duties and responsibilities of computer personnel should be segregated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be separated include application and system programming, quality assurance, computer operations, and data security. In addition, organizations with limited resources to segregate duties should implement compensating controls, such as reviewing recorded transactions, to mitigate the resulting risks. However, VA's OIG reported that computer duties were not appropriately separated at the Hines and Philadelphia benefits delivery centers.

System programmers at both the Hines and Philadelphia benefits delivery centers were also allowed to perform security administration functions. For example, VA's OIG found that security administrators at Hines had performed fewer than 60 of about 4,800 actions to administer security during a particular period. Because these individuals had both system and security administration privileges, they had the ability to improperly modify or delete data and programs and eliminate any evidence of their activity in the system. The risk of improper payments resulting from unauthorized modification to sensitive compensation, pension and insurance data maintained at these centers was also increased because neither center was monitoring user access activity to identify and investigate unusual or suspicious actions.

In August 1999, VBA management told us that VBA would implement compensating controls to mitigate the risks associated with not fully separating the data security and system programming functions at the Hines and Philadelphia benefits delivery centers.

User ID and Password Management Controls Are Not Effective

It is also important to actively manage user IDs and passwords to ensure that users can be identified and authenticated. To accomplish this objective, organizations should establish controls to maintain individual accountability and protect the confidentiality of passwords. These controls should include requirements to ensure that IDs uniquely identify users; passwords are changed periodically, contain a specified number of characters, and are not common words; default IDs and passwords are changed to prevent their use; and the number of invalid password attempts is limited to preclude password guessing. Organizations should also evaluate user ID and password management controls periodically to ensure that they are operating effectively.

Password management weaknesses persisted at VBA and VHA facilities. VA's OIG determined that users at both the Hines and Philadelphia benefits delivery centers were allowed to create passwords that were common words. A VHA consultant study also found that most VHA network passwords were easily guessed. Because the confidentiality of user IDs is typically not protected, allowing easily guessed passwords increases the risk that unauthorized users could gain access to VBA and VHA systems. A program for periodically testing password contents could have allowed these facilities to identify and eliminate easily guessed passwords.

In August 1999, VBA management told us that the benefits delivery centers were in the process of strengthening password management controls. For instance, the Hines BDC had conducted security awareness training on password management and the Philadelphia BDC had provided its employees guidance on effective password management.

In addition, VA's OIG reported that the security software was implemented in a manner that allowed unlimited guessing of the master security account, which has the highest level of security authority, at the Hines BDC. Allowing unlimited password attempts to this ID increases the risk of unauthorized access to or disclosure of sensitive benefit information maintained at Hines.

User Access Activity Was Not Adequately Monitored

The risks created by these control problems were also heightened because VA was not adequately monitoring user access activity. Such a 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 these resources. A comprehensive user access activity monitoring program is critical to ensuring improper access to sensitive information would be detected.

VA facilities had not yet implemented comprehensive user access activity monitoring programs. AAC was 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 addition, VA's OIG reported that neither the Hines nor Philadelphia benefits delivery centers had established programs to regularly monitor user access activities on the mainframe or network. Further, in its response to a MISS follow-up survey concerning recommendations in our September 1998 report, the Albuquerque medical center indicated that it had not established a targeted monitoring program for its telecommunications system. Until VA facilities begin adequately monitoring user access activity, the department will have little assurance that unauthorized access to financial and sensitive veteran medical and benefit information will be detected.

In May 1999, VA stated that AAC would complete its procedures for monitoring successful access to sensitive computer resources by the end of September 1999. In addition, VBA management told us in August 1999 that both the Hines and Philadelphia benefits delivery centers had begun monitoring user access activity.

Departmentwide Computer Security Planning and Management Is Essential

In September 1998, we reported that a primary reason for VA's information system control problems was that the department did not have a comprehensive computer security planning and management program to ensure that effective information system controls were established and maintained. VA has taken important steps to strengthen its computer security planning and management by establishing a centralized computer security group that reports directly to the department's CIO and developing a plan to establish a strong departmentwide information security program. As VA implements its computer security planning and management program, developing detailed guidance can help ensure that requirements

of the information security program are implemented fully and consistently throughout the department.

Planned Improvements Are Consistent With Our Security Management Framework

In our May 1998 study of information security best practices, we reported that central coordination of computer security planning and management programs is important in highly interconnected computing environments to ensure that weaknesses in one facility do not place the entire organization's information assets at unnecessary risk. In order to be effective, the central security focal point must have the authority to enforce the organization's security policies or have access to senior executives who can act and effect change across organizational divisions. One approach for ensuring that a central group has such access is to place it under a CIO who reports directly to the head of the organization. This approach is consistent with the Clinger-Cohen Act,[10] which requires that major federal departments and agencies establish CIOs who report to the department/agency head and are responsible for implementing effective information management.

In July 1998,[11] we reported that VA's CIO responsibilities were not limited primarily to information management. In response to this report, VA established an Assistant Secretary position, which reports directly to the Secretary of Veterans Affairs on all information resources issues, to serve as the department's CIO. To further strengthen its departmentwide computer security management program, in February 1999, VA established a centrally managed security group, which reports directly to the department's acting CIO, to provide policy, direction, and oversight for security management throughout the department. In March 1999, VA also chartered an Information Security Working Group, which includes representatives from the central security group and all VA line and staff organization security groups. This group finalized a multiyear plan in May 1999 to improve information system security and establish a departmentwide computer security planning and management program.

The information security program plan, which is to be phased in over several years, generally includes requirements for the key elements we believe to be important to having an effective security management

[10]The 1996 Clinger-Cohen Act, Public Law No. 104-106, section 5125, 110 Stat. 684 (1996).

[11]*VA Information Technology: Improvements Needed to Implement Legislative Reforms* (GAO/AIMD-98-154, July 1998).

program–establishing guidance and procedures for assessing risk, implementing appropriate policies and controls, raising awareness of prevailing risks, and monitoring and evaluating the effectiveness of established controls. The plan also (1) defines the roles and relationships of the principle stakeholders in VA's information security program and (2) sets milestones for specific tasks defined in the planned security initiatives that were developed to accomplish security program plan requirements. However, because the information security program plan is at an early stage of development and is not scheduled to be fully implemented until January 2003, it is too soon to assess its ultimate effect on improving information security throughout VA.

The success of VA's efforts to improve departmentwide computer security planning and management will depend largely on adequate resources being dedicated to its information security program plan and on the level of commitment throughout the department to effectively implement the requirements of this plan. Although the plan recognizes that dedicated staff and recurring funds are critical, VA has not yet approved funding requested to implement the information security program plan over the next several years. In addition, the acting VA CIO is still obtaining formal concurrence with the information security program plan from other key VA organizations, including the three VA administrations and the Office of Financial Management. Including representatives from all levels in developing the information security program plan should help foster support for the plan and the associated security initiatives. However, as VA implements its information security program, it will be important to monitor compliance with departmentwide security policies and guidance to determine if additional mechanisms, such as performance measures that hold program managers accountable for information security, are required to help ensure that requirements of the program are fully implemented throughout the department. To be effective, the acting CIO must have the authority to enforce VA's security policies or access to the Secretary of Veterans Affairs to ensure that needed changes can be implemented across VA organizations.

Comprehensive Policies and Guidance Are Important to Ensure Consistent Implementation

Our May 1998 study of security management best practices found that current, comprehensive security policies, which cover all aspects of an organization's interconnected environment, are important because written policies are the primary mechanism by which management communicates its views and requirements. We also reported that organizations should develop both high-level organizational policies, which emphasize

fundamental requirements, and more detailed guidelines or standards, which describe an approach for implementing policy. Such guidance not only helps ensure that appropriate information system controls are established consistently throughout the department, but also facilitates periodic reviews of these controls.

VA's plan includes an initiative to develop, with significant involvement from affected organizations, a security policy framework by September 1999 and an updated umbrella policy by March 2000. Also, technology-specific security policies, which should establish technical security standards for the various VA computing environments, are to be developed by October 2000. As VA implements its security policy, developing detailed guidance will help ensure that key program elements are fully addressed and implemented consistently across the department. In September 1998, we reported weaknesses at VA in key information security areas such as performing risk assessments, monitoring user access activities, and monitoring and evaluating the effectiveness of the security program. To help correct these weaknesses, VA's detailed guidance should include provisions as discussed below.

Guidance for Assessing Risk

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 to 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 managing risk on a continuing basis.

Managing risk relating to computer security on a continuing basis is especially important because computer systems and the environments in which they operate change continually. Although VA's security policy requires risk to be assessed when significant changes are made to a facility or its computer systems, it does not provide additional guidance for determining if an event is a significant change or address risk analysis requirements for other changes. Although many changes made to computer systems are not significant and do not require extensive risk analyses, security risks associated with these changes should still be considered. These risk assessments could be very limited and informal, but should still be appropriately documented. For example, replacing a mainframe computer and implementing a new mainframe operating system would be considered a significant change requiring a formal risk assessment;

whereas, the risk assessment for changes such as updating system software or adding a network server configured similar to others already in use could be more informal.

In addition, VA's departmentwide security handbook did not provide additional guidance for conducting risk assessments. In our May 1998 study of security management best practices, we found that it was important for organizations to define a risk assessment process that could be adapted to different organizational units and involve individuals with knowledge of business operations, security controls, and the technical aspects of the applicable computer systems. In our study of risk assessment best practices,[12] we also reported that procedures for conducting risk assessments generally specified

- how risk assessments should be initiated and conducted,
- who should participate in the risk assessment,
- how disagreements should be resolved,
- what approvals were needed, and
- how assessments should be documented and maintained.

Framework for Monitoring System and User Access Activity

To ensure that unauthorized attempts to access sensitive information are detected, organizations should develop guidance for monitoring system and user access activity and investigating possible security incidents. This includes network monitoring to promptly identify potential security incidents, and examining user access activity to identify unauthorized attempts, both successful and unsuccessful, to access VA systems.

A proactive network monitoring program would allow VA to promptly identify and investigate unusual or suspicious network activity indicative of malicious, unauthorized, or improper attempts to access or disrupt VA systems. Such a program would require VA to (1) identify suspicious access patterns, such as repeated failed attempts to log on to the network, attempts to identify systems and services on the network, connections to the network from unauthorized locations, and efforts to overload the network to disrupt operations, and (2) set up an intrusion detection system to automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

[12] *Information Security Risk Assessment: Practices of Leading Organizations*, Exposure Draft (GAO/AIMD-99-139, August 1999).

In addition to identifying attempts by unauthorized users to gain access to the system, it is also important to monitor attempts to access sensitive information once entry to the system is accomplished. Routinely monitoring the access activities of users to identify and investigate unusual or suspicious access to sensitive data and resources could help identify significant problems and deter employees from inappropriate and unauthorized activities.

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, including security software, system software, application programs, and production data. This would include evaluating both failed attempts to access sensitive data and resources, as well as successful access to these resources exhibiting unusual or suspicious activity, 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 financial and sensitive veteran medical and benefit data.

VA could develop such a program by (1) identifying sensitive system files, programs, and data files on its computer systems and the network, (2) using the audit trail capabilities of its security software to document both failed and successful access to these resources, (3) defining normal patterns of access activity, and (4) analyzing audit trail information to identify and report on access patterns that differ significantly from defined normal patterns.

Program for Monitoring and Evaluating the Effectiveness of Information System Controls

It is also important for information system controls to be monitored and periodically reassessed to ensure that policies continue to be appropriate and that controls are accomplishing their intended purpose. Over time, policies and procedures may become inadequate because of changes in threats, changes in operations, or deterioration in the degree of compliance. Periodic assessments or reports on activities can be a valuable means of identifying areas of noncompliance, reminding employees of their

responsibilities, and demonstrating management's commitment to the security program. 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 and (2) testing the effectiveness of information system controls. Performing these processes is a key step in the cycle of managing information security.

In the VA environment, periodic security self-assessments and independent security reviews could be used to monitor compliance with established information system control policies and guidelines. For example, periodically reviewing user access authority to ensure that it is limited to the minimum required access level based on job requirements would allow VA organizations to discover and correct access control weaknesses. Likewise, setting technical security standards for system software and routinely evaluating the technical implementation of the system software based on these standards would permit VA to eliminate or mitigate system software exposures. Also, software tools such as password crackers could be used to monitor compliance with VA password guidelines that prohibit the use of English words.

In addition to monitoring, directly testing information system controls would allow VA to determine if the risk reduction techniques that had been agreed to are, in fact, operating effectively. For example, periodically (1) running computer programs designed to detect vulnerabilities in VA's network environment and (2) allowing designated individuals to try to "break into" VA systems using the latest hacking techniques could be used to test the effectiveness of information system controls throughout VA. By allowing such tests, VA could readily identify previously unknown vulnerabilities and either eliminate them or make adjustments to lessen risks. Our May 1998 study also found that unannounced tests of disaster recovery plans had been successful in identifying plan weaknesses and in dramatically sensitizing employees to the value of anticipating and being prepared for such events.

Although monitoring and testing information system controls may encourage compliance with information security policies, the full benefits of these actions are not achieved unless results are used to improve the security program. Analyzing the results of these efforts provides a means of reassessing previously identified risks, identifying new problem areas, reassessing the appropriateness of existing controls, identifying the need for new controls, and redirecting subsequent monitoring and testing

efforts. The VA central security group had begun monitoring the status of actions to remedy findings reported in external information security audits conducted by GAO and VA's OIG. However, the quarterly Security Audit Remediation Report did not track weaknesses identified by internal management or consultant security studies. Also, the corrective actions included in the Security Audit Remediation Report for GAO reviews are based on recommendations rather than the underlying weaknesses. Therefore, it is not always evident if the specific weaknesses that prompted our recommendations have been addressed. Furthermore, VA did not have a process in place to ensure that reported corrective actions are operating as intended.

In addition to monitoring and testing controls, periodically analyzing security incidents can identify vulnerabilities and security problems that need to be addressed. Keeping summary records of actual security incidents is one way that an organization can measure the frequency of various types of violations as well as the damage suffered from these incidents. One of the organizations we studied in our May 1998 report on security management best practices developed an incident database that served as a valuable management tool in monitoring problems, reassessing risks, and determining how to best use limited resources to address the most significant problems. By keeping a record of incidents, the organization could develop monthly reports that showed increases and decreases in incident frequency, trends, and the status of resolution efforts. These reports provided the organization a means of identifying emerging problems, assessing the effectiveness of current policies and awareness efforts, determining the need for stepped up education or new controls to address problem areas, and tracking corrective actions.

Conclusions

Although VA organizations, especially AAC, had independently taken actions to correct some of the weaknesses we reported in September 1998 and improve local computer security planning and management programs, these efforts were not coordinated as part of a departmentwide effort. Consequently, improvements in computer security were inconsistent across VA organizations and VA's computer systems, programs and data continued to be vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection.

VA has recently taken important steps to strengthen its computer security planning and management program by developing a plan to improve

information security throughout the department and establishing a central security group, which reports directly to the acting CIO, to provide overall policy, direction, and oversight. VA's Information Security Program Plan includes requirements that address the key elements of our computer security planning and management framework. However, because this multiyear plan is at an early stage of development, it is too soon to assess its impact on VA efforts to establish and maintain effective information system controls.

The success of VA's actions to improve information security will depend largely on adequate resources being effectively dedicated to implement its information security program plan and the level of commitment throughout the department to improve information security. To be effective, the central security group must have the authority to enforce VA's security policies or have access to the Secretary of Veterans Affairs to ensure that needed changes can be implemented across VA organizations. In addition, as VA implements its departmentwide computer security planning and management program, it will be important to develop detailed guidance to ensure that key program elements, such as periodically assessing risk, monitoring system and user access activity, evaluating compliance with security policies and guidelines, and testing the effectiveness of information system controls, are fully addressed and implemented consistently across the department.

Recommendations

We recommend that the Secretary of Veterans Affairs direct the VA CIO to

- periodically report to the Secretary on progress in implementing its information security program plan;
- develop detailed departmentwide guidance and oversight processes as described in this report so that important aspects of computer security programs, such as periodically assessing risks, monitoring system and user access activity, and monitoring and evaluating information system policy and control effectiveness, are fully addressed and implemented consistently throughout the department; and
- expand the scope of current procedures for tracking information security weaknesses so that all information security weaknesses identified by management, consultants, the audit community, or other external organizations are included and that reported corrective actions are operating as intended.

Agency Comments

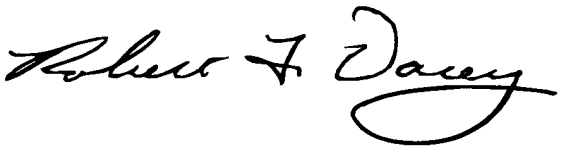
In commenting on a draft of this report, VA agreed with our recommendations. Specifically, VA stated that the CIO will periodically report to the Secretary on progress in implementing the information security program. VA stated that it plans to integrate this reporting into a single, coherent executive reporting framework that will include FMFIA and PDD-63 reporting requirements. In addition, VA stated that the CIO will develop detailed processes for assessing risks, monitoring system access activity, and monitoring and evaluating information system policy and control effectiveness as part of a departmentwide security policy framework to be completed by October 2000. Finally, VA stated that the CIO will expand ongoing reporting on progress to remedy each specific weakness to the VA OIG and include other computer security weaknesses as they surface.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations. You should send your statement to the Senate Committee on Governmental Affairs and the House Committee on Government Reform within 60 days of the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made over 60 days after the date of this report.

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 a copy to 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 or Dave Irvin at (214) 777-5716. Key contributors to this assignment were Shannon Cross, Jeffrey Knott, and Charles Vrabel.

Sincerely yours,



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

Comments From the Department of Veterans Affairs

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF VETERANS AFFAIRS
ASSISTANT SECRETARY FOR PLANNING AND ANALYSIS
WASHINGTON DC 20420

SEP 0 2 1999

Mr. Jeffrey C. Steinhoff
Acting Assistant Comptroller General
Accounting and Information Management Division
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Steinhoff,

See comment 1.

We have reviewed your draft report, ***INFORMATION SYSTEMS: The Status of Computer Security at the Department of Veterans Affairs*** (GAO/AIMD-99-253) and offer these comments. The Department is keenly interested in its information security program and puts a high priority on the safeguarding of our electronic data as well as the physical protection of our operational centers. We concur with GAO's recommendations and believe that they will lead to an overall improvement of VA's information systems security program.

The enclosure details actions we have planned and taken to implement your recommendations. Thank you for the opportunity to comment on your draft report.

Sincerely,

Dennis Duffy

Enclosure

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS TO
GAO DRAFT REPORT, ***INFORMATION SYSTEMS:***
The Status of Computer Security at the Department of Veterans Affairs
(GAO/AIMD-99-253)

GAO recommends that the Secretary of Veterans Affairs direct the VA CIO to:

- **periodically report to the Secretary on progress in implementing its information security program plan;**

Concur – VA's CIO is already required to report at least semi-annually on information security under the FMFIA material weakness program. The CIO, in partnership with the Department's Chief Infrastructure Assurance Officer (CIAO), will also be required to report periodically on progress in meeting the PDD-63 deadline of May 2003 to have a full operating capability for protection of critical infrastructure. The CIO will periodically report his progress in implementing the information security program to the Secretary until we have achieved our goal of a single, coherent executive reporting framework to serve all these demands.

- **develop detailed departmentwide guidance and oversight processes as described in this report so that important aspects of computer security programs, such as periodically assessing risks, monitoring system and user access activity, and monitoring and evaluating information system policy and control effectiveness, are fully addressed and implemented consistently throughout the department; and**

Concur – VA's CIO will develop these control processes in a way that effectively embeds them into a revamped security policy framework. The multi-year security program plan that the CIO has coordinated across the Department sets a completion date of October 2000 for this policy framework. The CIO will monitor and evaluate Departmental, and VA Administration and Staff Office, information security program effectiveness and compliance with statutes, regulations, and VA policy.

- **expand the scope of current procedures for tracking information security weaknesses so that all information security weaknesses identified by management, consultants, the audit community, or other external organizations are included and that reported corrective actions are operating as intended.**

1

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS TO
GAO DRAFT REPORT, ***INFORMATION SYSTEMS:***
The Status of Computer Security at the Department of Veterans Affairs
(GAO/AIMD-99-253)

(Continued)

Concur - One recommendation of the earlier GAO audit, ***INFORMATION SYSTEMS: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure*** (AIMD-98-175) required VA's CIO to review and assess computer control weaknesses that were identified throughout the department, and to establish a process to ensure that these weaknesses were addressed. In implementing this recommendation, VA's CIO reports regularly to the Office of Inspector General on the progress to remedy each specific weakness. The CIO has not constrained this report by any artificially defined scope and will expand it to embrace any additional weaknesses that surface as a result of further examinations of computer controls.

2

The following is GAO's comment on the Department of Veterans Affairs letter dated September 2, 1999.

GAO Comment

1. The report number has been changed to GAO/AIMD-00-5.

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