United States General Accounting Office

GAO

Report to the Acting Secretary of Veterans Affairs

September 2000

VA INFORMATION SYSTEMS

Computer Security Weaknesses Persist at the Veterans Health Administration

GAO

Accountability * Integrity * Reliability

GAO/AIMD-00-232

Contents

Letter 3

Appendixes

Appendix I: Comments From the Department of Veterans Affairs 34

Appendix II: Computer Security Weaknesses We Identified at Three VHA Health Care Systems 39

Appendix III: GAO Contact and Staff Acknowledgements 42

Abbreviations

AAC	Austin Automation Center
CIO	chief information officer
FMFIA	Federal Managers' Financial Integrity Act of 1982
ID	identification
IRM	Information Resource Management
ISO	information security officer
NMVAHCS	New Mexico VA Health Care System
OIG	office of inspector general
VA	Department of Veterans Affairs
VA-CIRC	VA's critical incident response capability
VAMHCS	VA Maryland Health Care System
VANTHCS	VA North Texas Health Care System
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

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

Accounting and Information
Management Division

B-285729

September 8, 2000

The Honorable Hershel W. Gober
The Acting Secretary of Veterans Affairs

Dear Mr. Secretary:

We reviewed information system general controls[1] over financial and sensitive veteran medical information maintained by the Veterans Health Administration (VHA) in connection with the Department of Veterans Affairs' (VA) required annual consolidated financial statement audit[2] for fiscal year 1999. The purpose of this report is to advise you of the status of computer security within VHA and initiatives to improve computer security throughout the department.

As part of our review, we assessed computer security at the VA Maryland Health Care System, the New Mexico VA Health Care System, and the VA North Texas Health Care System. Our evaluation included follow-up on (1) specific computer security weaknesses we identified at the New Mexico and North Texas health care systems in conjunction with the audit of VA's fiscal year 1997 financial statements[3] and (2) departmentwide computer security initiatives that we reported in October 1999.[4] We issued separate letters to the directors of the three health care systems that detail the results of our reviews and include recommendations to correct the security

[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 23, 1998).

[4]*Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4, 1999).

weaknesses we identified.[5] The results of our underlying reviews were also shared with VA's Office of Inspector General (OIG) for its use in auditing VA's consolidated financial statements for fiscal year 1999.

Results in Brief

In September 1998, we reported that computer security weaknesses placed critical VA operations, including health care delivery, at risk of misuse and disruption.[6] Since then, VA's New Mexico and North Texas health care systems have corrected most of the specific computer security weaknesses that were identified in 1998. However, serious computer security problems persist throughout VHA and the department because (1) VA had not yet fully implemented an integrated security management program and (2) VHA had not devoted adequate resources to effectively manage computer security at its medical facilities. Consequently, financial transaction data and personal information on veteran medical records continue to face increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection.

We identified additional computer security problems at the New Mexico and North Texas health care systems and also found similar serious weaknesses at the VA Maryland Health Care System. These medical facilities had not adequately controlled access granted to authorized users, prevented employees from performing incompatible duties, secured access to networks, restricted physical access to computer resources, or ensured the continuation of computer processing operations in case of unexpected interruption. The access and service continuity weaknesses we found are similar to problems consistently identified since 1998 at VHA medical facilities by VA's OIG, internal VHA reviews, and consultant studies.

VA's OIG has reported departmentwide information system security as a material internal control weakness since the fiscal year 1997 consolidated financial statement reporting period. VA recognized the significance of these problems and began reporting information system security as a

[5] *VA Systems Security: Information System Controls at the VA Maryland Health Care System* (GAO/AIMD-00-117R, April 19, 2000*); VA Systems Security: Information System Controls at the New Mexico VA Health Care System* (GAO/AIMD-00-88R, March 24, 2000); and *VA Systems Security: Information System Controls at the North Texas Health Care System* (GAO/AIMD-00-52R, February 1, 2000).

[6] GAO/AIMD-98-175, September 23, 1998.

material weakness in its Federal Mangers' Financial Integrity Act of 1982 (FMFIA)[7] report for 1998.

One reason for VA's continuing information system control problems is that the department had not implemented a comprehensive, integrated security management program. In October 1999, we reported that VA had established a central security group and developed an information security program plan that generally addressed the key elements of effective computer security management programs.[8] Since then, VA has made progress in meeting several security program plan milestones, but had not yet developed detailed guidance to ensure that key information security areas highlighted in our October 1999 report—assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls—are fully addressed and consistently implemented throughout the department. Initiating a process to review and build on security practices developed by other VA organizations could expedite VA efforts to develop departmentwide guidance in these areas.

In October 1999, we also reported that VA's success in improving computer security was largely dependent on the level of commitment throughout the department and adequate resources being effectively dedicated to implement the proposed plan. However, VHA had not yet committed resources that are critical to VA's ability to continue to develop and implement an effective departmentwide computer security program. In addition, VHA had not adequately staffed information security officer (ISO) positions responsible for security oversight at VA medical facilities. Until VA develops and implements a comprehensive, coordinated security management program and ensures that adequate resources are devoted to this program, it will have limited assurance that financial information and sensitive veteran medical records are adequately protected from misuse, unauthorized disclosure, and/or destruction.

To improve computer security at VHA medical facilities, we are making recommendations to correct the computer security weaknesses we identified at the health care systems we visited and provide security oversight resources to effectively manage computer security at VHA

[7]FMFIA requires agencies to establish controls that reasonably ensure that assets are safeguarded against waste, loss, or unauthorized use.

[8]GAO/AIMD-00-5, October 4, 1999.

medical facilities. To facilitate VA efforts to develop and implement a comprehensive, coordinated security management program that would encompass VHA and other VA organizations, we are also reaffirming our October 1999 recommendation for VA to develop detailed computer security guidance and oversight processes and making an additional recommendation to monitor and resolve coordination issues that could affect the success of the departmentwide computer security program.

In commenting on this report, VA concurred with all our recommendations. The Acting Secretary of Veterans Affairs stated that he was concerned with the information system security weaknesses we identified and, therefore, was instructing the acting CIO to develop an accelerated plan to improve information system controls at VA facilities.

Background

VA is responsible for administering health care and other benefits that directly affect the lives of more than 25 million veterans and approximately 44 million members of their families. To provide health care services, VHA operates one of the largest health care delivery systems in the United States and also conducts research and education. In fiscal year 1999, VA reported spending around $17.5 billion to provide medical care to more than 3 million veterans. Such care is managed through 22 Veterans Integrated Service Networks (VISN), which are geographically dispersed throughout the country. These VISNs oversee more than 800 medical facilities—including 172 medical centers, 519 outpatient clinics, 134 nursing homes, and 40 domiciliaries—that provide a broad range of medical, surgical, and rehabilitative care. In some cases, different types of medical facilities, such as medical centers and outpatient clinics, are collectively referred to as a health care system within a VISN. For example, the New Mexico VA Health Care System consists of a medical center located in Albuquerque, New Mexico, and community-based outpatient clinics located in rural communities throughout New Mexico. The New Mexico VA Health Care System is combined with four other health care systems, one medical center, one independent outpatient clinic, six nursing homes, and one domiciliary into the Southwest Network, a designated VISN.

In providing health care services, VHA collects and maintains sensitive medical records for veteran inpatient and outpatient care through a collection of standard medical, administrative, and financial computer applications used by its medical facilities. For example, VHA stores admission, diagnosis, surgical procedure, and discharge information for each stay in a VA medical center, nursing home, or domiciliary. Each of the

172 VA medical centers, which are located around the country, processes these standard applications on local computer systems.

In addition, VHA's standard administrative and financial applications control most of the approximately $17.5 billion that VA reported spending on medical care in fiscal year 1999. Almost $10.5 billion of this $17.5 billion was managed through the Personnel and Accounting Integrated Data system. Most of the remaining $7 billion was initiated through VHA's main financial system—the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement system.

VHA relies on telecommunications networks to support its operations and store and communicate sensitive medical information. For example, some medical facilities operate independent systems, such as medical imaging and patient monitoring systems, that link to standard medical applications at the facility through local area networks. In addition, local area networks at VHA customer organizations, such as non-VHA hospitals and medical universities, are connected to local area networks at VHA medical facilities through a combination of VHA and VA wide area networks. Furthermore, several of VHA's standard medical and administrative systems transmit financial and sensitive medical information to VA departmentwide systems, which are maintained at the Austin Automation Center (AAC), through VA's wide area network.

VA's network not only connects local area networks at VHA medical facilities to customer organizations and the departmental data center in Austin, Texas, but also provides links to the Veterans Benefits Administration's (VBA) centralized data centers in Hines, Illinois, and Philadelphia, Pennsylvania, the 58 VBA regional offices, and VA headquarters. 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 within VHA and evaluate departmentwide initiatives to improve computer security throughout VA. To determine the status of computer security within VHA, we (1) evaluated information system general controls at the VA Maryland Health Care System, the New Mexico VA Health Care System, and the VA North Texas Health Care System and (2) reviewed VA's fiscal year 1999 financial statement audit report; VA's 1999 FMFIA report; and VA OIG, internal VHA, and consultant reports on computer security at VHA facilities. We restricted our review of information system general controls

to selected VHA medical facilities because VA's OIG planned to evaluate these controls at VBA and other VHA facilities as part of the department's fiscal year 1999 financial statement audit.

To evaluate information system general controls at the Maryland, New Mexico, and North Texas health care systems, we identified and reviewed general control policies and procedures. We also tested and observed the operation of information system general controls at these medical facilities to determine whether controls were in place, adequately designed, and operating effectively. Our evaluation was based on our *Federal Information System Controls Audit Manual*,[9] 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 computer security weaknesses we had previously identified at the New Mexico and North Texas health care systems. We requested and received comments on the results of our evaluation from the directors of each medical facility we visited. We did not verify VA statements regarding corrective actions taken subsequent to our site visits, but plan to do so during future reviews.

To determine the status of departmentwide security initiatives, we held discussions with VA officials and reviewed current as well as planned computer security policies and initiatives. Our evaluation was based on the results of our May 1998 study of security management best practices at leading organizations,[10] which identifies key elements of effective information security program management. 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 Chief Information Officers (CIO) Council. We performed our work from October 1999 through July 2000, in accordance with generally accepted government auditing standards.

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

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

We requested written comments on a draft of this report from the Acting Secretary of Veterans Affairs or his designee. VA provided us with written comments which are discussed in the "Agency Comments" section and reprinted in appendix I.

Information in VHA Systems Was Still Vulnerable to Misuse and Disruption

In September 1998, we reported that computer security weaknesses placed critical VA operations, including health care delivery, at risk of misuse and disruption.[11] Although the New Mexico and North Texas health care systems had corrected most of the specific computer security weaknesses that were identified in 1998, we found additional information system control problems at these medical facilities. At the VA Maryland Health Care System, we also identified serious computer security weaknesses, which were similar to the problems identified at the New Mexico and North Texas health care systems. Specifically, the VHA health care systems we visited had not adequately controlled access granted to authorized users, limited access to prevent employees from performing incompatible duties, secured access to networks, restricted physical access to computer resources, or ensured the continuation of computer processing operations in case of unexpected interruption. Consequently, financial transaction data and personal information on veteran medical records are still vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection.

Management officials at the VHA health care systems we visited acknowledged the computer security weaknesses we identified and expressed a commitment to improving information system controls. Subsequent to our fieldwork, each facility provided us with an action plan that included updated information regarding corrective actions taken and plans to address all remaining open weaknesses. We did not verify that the reported corrective actions had been implemented but plan to do so as part of future reviews. Proper implementation of the action plans provided should correct all previously identified security issues.

Appendix II describes the computer security weaknesses that remained at the completion of our 1999 site visits. The following sections summarize the results of our reviews of the Maryland, New Mexico, and North Texas health care systems.

[11]GAO/AIMD-98-175, September 23, 1998.

New Mexico and North Texas Health Care Systems Had Corrected Most Previously Identified Weaknesses

Both the New Mexico and North Texas health care systems had made substantial progress in addressing the specific computer security issues we previously identified. At the time of our review in 1999, the New Mexico VA Health Care System had corrected 15 of the 22 issues that we discussed with the director and summarized in our September 1998 report on VA computer security. [12] Similarly, the VA North Texas Health Care System had corrected 19 of the 23 issues that we previously identified and summarized in the same September 1998 report. Both of these medical facilities had addressed most of the access control, application change control, and service continuity weaknesses we identified in 1997. For example, both health care systems had

- reduced the number of users with access to the computer room,
- corrected the password control weaknesses we identified,
- developed procedures to review changes to standard VHA applications, and
- established processes to periodically review disaster recovery plans.

In addition, the VA North Texas Health Care System had appointed a full-time ISO since our last visit and had established a foundation for implementing a computer security management program. Subsequent to our site visits, the Maryland and New Mexico health care systems also appointed full-time ISOs to help improve computer security.

Despite these efforts, we identified additional computer security problems at the New Mexico and North Texas health care systems and also found similar serious weaknesses at the VA Maryland Health Care System.

Access Authority Was Not Appropriately Controlled

A key weakness in internal controls was that medical facilities we visited were not appropriately controlling access to sensitive data and programs associated with standard VHA medical and financial applications. To provide reasonable assurance that these resources are protected against inappropriate modification or disclosure, organizations should (1) grant employees authority to read or modify only those programs and data that are necessary to perform their duties, (2) periodically review this authority and modify it to reflect changes in job responsibilities, and (3) monitor

[12] GAO/AIMD-98-175, September 23, 1998.

access activity to ensure that access authorities are being used appropriately.

None of the health care systems we visited were adequately controlling powerful user identifications (ID) capable of accessing all financial and sensitive veteran medical information. While it is appropriate for selected computer staff to have this broad access authority, the number of staff given access to all financial and sensitive veteran medical information should be limited and adequately controlled. However, the health care systems we visited had not set up control mechanisms to ensure that (1) access authorizations for IDs capable of accessing all financial and sensitive veteran information were required and maintained or (2) IDs with broad access authority were periodically reviewed to determine if this level of access remained appropriate. In addition, none of the health care systems we visited were routinely monitoring access activity for user IDs with broad access authorities to determine if these user IDs were being used only for their intended purposes.

Subsequent to our review, officials at the New Mexico and North Texas health care systems told us that procedures for controlling user IDs with broad access authority to all financial and sensitive veteran medical information had been implemented. In addition, VA Maryland Health Care System officials stated that such procedures would be implemented by September 2000.

Employees Were Not Prevented From Performing Incompatible Duties

In addition to controlling user access authority, it is important to grant access authority in a manner that restricts employees from performing incompatible functions. Segregating incompatible duties reduces the risk that errors or fraud will occur and go undetected. However, the Maryland and New Mexico health care systems had not restricted access to prevent employees from performing incompatible procurement functions.

At both of these medical facilities, more than 10 staff involved with procurement had been granted access authority that allowed them to request, approve, and receive medical items without management approval. This violates basic segregation of duties principles and VA policy. We also determined that staff members at the New Mexico VA Health Care System had requested, approved, and received 60 purchases totaling about $300,000 in medical-related supplies from October 1998 through November 1999. However, we found no evidence of management approval of these purchases as prescribed by VHA policy, nor did we find mitigating controls

to alert management of purchases made in this manner. Allowing fiscal agents to have total control of purchases increases the risk that inappropriate or fraudulent transactions could be processed without detection.

In February 2000, New Mexico VA Health Care System officials told us that they had reviewed the 60 purchases and found no evidence of fraud or abuse. In July 2000, New Mexico VA Health Care System officials also told us that they had (1) implemented policies to limit the number of users capable of requesting, approving, and receiving items and (2) established procedures to monitor the purchasing activity of users who have this level of access. In addition, VA Maryland Health Care System officials told us that they would implement similar procedures by the end of August 2000.

Network Security Was Not Sufficient

It is also essential to protect access to VHA networks and other systems connected to VHA networks. However, the VHA health care systems we visited had not adequately managed network user IDs and passwords, restricted access to network operating system software, or monitored network system activity. While these network security weaknesses would not have a direct impact on the financial and sensitive veteran medical information maintained in VHA's standard applications, network security weaknesses increase the risk of unauthorized access to these and other VA systems that are connected to the network.

Network ID and Password Management

It is 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 different types 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 these controls periodically to ensure that they are operating effectively. At the three health care systems we visited, network user IDs and passwords were not being effectively managed to ensure individual accountability and reduce the risk of unauthorized access.

At the time of our site visits, VA guidance required network users to have separate IDs; passwords that were changed periodically, at least six characters in length, and formed with other than common words; and IDs

to be suspended after three invalid password attempts. Despite these requirements, network ID and password management weaknesses persist because none of the health care systems we visited were reviewing user IDs and passwords for compliance with VA guidance. For instance, passwords for user IDs on Maryland and New Mexico networks were not prevented from being less than six characters in length. Network system parameters at the VA Maryland Health Care System did not require minimum password lengths and the minimum password length on the New Mexico VA Health Care System network was set to two characters. This allows users to establish very short passwords that are more easily guessed than longer passwords. In addition, 94 IDs on the VA Maryland Health Care System network were especially susceptible to misuse because passwords were not required.

We also found that the three health care systems we visited were not promptly removing access authority for terminated employees or deleting unused or unneeded IDs. For example, over 120 North Texas, 59 New Mexico, and 45 Maryland network user IDs belonged to terminated employees. If user IDs are not promptly disabled when employees are terminated, former employees are allowed the opportunity to sabotage or otherwise impair VA operations. This also introduces unnecessary risk that unneeded IDs will be used to gain unauthorized access to VA computer resources.

Subsequent to our fieldwork, officials at each of the three health care systems we visited told us that their staffs, working with other VA organizations as needed, had either corrected or planned to correct the network ID and password management weaknesses we identified by September 2000.

Network System Software

Organizations must also control access to and modification of system software to protect the overall integrity and reliability of information systems. System software controls, which limit and monitor access to the powerful programs and sensitive files associated with computer system operations, are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. If controls in this area are not adequate, system software might be used to bypass security controls or gain unauthorized privileges that allow improper actions or the circumvention of edits and other controls built into application programs. However, the VHA health care systems we visited were not properly controlling network system software to prevent access controls from being circumvented or the system from being disrupted.

We identified system software configuration weaknesses that could allow users to bypass access controls and gain unauthorized access to VHA networks or cause network system failures. For example, networks at each of the three VHA health care systems we visited were set up in a manner that permitted individuals to connect to the network without entering valid user ID and password combinations. This could allow unauthorized individuals to obtain access to system information describing the network environment, including user IDs, password properties, and account details, and target network administrator IDs with password-cracking software.

We also determined that the Maryland and New Mexico health care systems were not adequately restricting access to sensitive system directories, which could allow authorized users to compromise the integrity of the network operating system. Regardless of their job responsibilities and access needs, all users were granted a level of access that would allow them to change or delete critical system information. In addition, all New Mexico VA Health Care System users had access to certain network system settings that would allow them to create or set system parameters that could execute malicious code upon system start-up.

Subsequent to our fieldwork, officials at the three health care systems we visited told us that they had either corrected these weaknesses or were working with other VA organizations to address the network system software problems we identified by November 2000.

Network Security Monitoring

The risks created by these network access control problems were exacerbated because none of the three VHA health care systems we visited had a proactive network monitoring program. Such a program would require a medical facility to promptly identify and investigate unusual or suspicious network activity indicative of malicious, unauthorized, or improper activity—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—to detect intrusions and misuse before significant damage occurs. Network monitoring programs should also include provisions for logging and regularly reviewing network access activities. Without these controls, VHA has little assurance that unauthorized access to systems on its networks would be detected in time to prevent or minimize damage.

None of the three health care systems we visited had established proactive network monitoring programs to identify unusual or suspicious activities.

Although the Maryland and North Texas health care systems had activated software that was capable of detecting attacks on a real-time basis, none of the three health care systems we visited had completed configuring intrusion detection systems to (1) identify suspicious access patterns and (2) automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

Also, none of the three health care systems we visited could ensure that network attacks would be detected after the fact because these medical facilities were not adequately monitoring network access activity. The three health care systems we visited had not established requirements for logging access to sensitive network data and resources or reviewing access to these resources for unusual or suspicious activity. Although each medical facility we visited was logging some network access activity, any unauthorized access to sensitive network data and resources was still likely to go undetected because these logs were not regularly reviewed.

In July 2000, North Texas Health Care System officials told us that a proactive network monitoring program to identify unusual or suspicious activity had been established and will be coordinated at the VISN level. Officials at the Maryland and New Mexico health care systems also told us that their staffs would work with VISN staff as necessary to develop and implement proactive network monitoring programs no later than November 2000. In addition, as part of its standard security infrastructure initiative, VA plans to implement a departmentwide intrusion detection system by November 2002.

Physical Security Controls Were Not Adequate

Physical security controls are also important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms where these resources are stored. At VHA facilities, physical access control measures, such as locks, guards, badges, and alarms (used alone or in combination), are critical to safeguarding critical financial and sensitive veteran medical information and computer operations from internal and external threats. However, we found weaknesses in physical security controls at each of the three VHA health care systems we visited.

None of the health care systems had developed formal procedures for granting and periodically reviewing access to the main computer room. As a result, staff could be granted access or continue to have access to

sensitive areas even though their job responsibilities may not warrant this access. For example, all staff in the VA Maryland Health Care System Information Resources Management office and two maintenance staff at the Baltimore Rehabilitation and Extended Care Center had keys to the computer room. While it is appropriate for some information resources management staff to have access to the computer room, care should be taken to limit access to only those employees who have a reasonable need. We also determined that a key to the New Mexico VA Health Care System computer room was assigned to an employee who no longer works at the health care system.

In April 2000, the director of the VA North Texas Health Care System told us that his staff had established policy and procedures for allowing, recording, and monitoring access to computer rooms. In July 2000, New Mexico Health Care System staff also told us that the physical security weaknesses we identified had been corrected, and VA Maryland Health Care System officials stated that they would correct the physical security weaknesses we identified by October 2000.

Service Continuity Planning Was Not Complete

In addition to protecting data and programs from misuse, organizations must also ensure that they are adequately prepared to cope with a loss of operational capability due to earthquakes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested service continuity plan. Such a plan is critical for helping to ensure that information system operations and data can be promptly restored in the event of a disaster. However, none of the three health care systems we visited had a complete and fully tested service continuity plan.

The Maryland and North Texas health care systems did not have complete service continuity plans. The VA Maryland Health Care System plan did not include detailed recovery procedures for each system, a priority order for system restoration, a list of key contacts and their responsibilities, requirements for testing the plan, or provisions for periodically reviewing and updating the plan. Likewise, the VA North Texas Health Care System plan did not include provisions for restoring all mission-critical systems, including its network systems. In addition, none of the health care systems we visited were fully testing their service continuity plans. The VA North Texas Health Care System was not performing annual testing as required by VA and VHA policy and the Maryland and New Mexico health care systems

were not performing periodic walk-throughs or unannounced tests of their plans.

North Texas Heath Care System officials told us that their staff had begun testing its service continuity plans and would complete service continuity plans for all its network systems by September 2000. Also, VA Maryland Health Care System officials told us that they would develop a new disaster recovery plan and begin testing it by the end of October 2000. Additionally, New Mexico VA Health Care System officials told us in July 2000 that their staff had begun performing quarterly walk-throughs of the system's service continuity plan.

Access Control and Service Continuity Weaknesses Were Widespread Throughout VHA

The access control and service continuity problems that we identified and describe in this report are similar to computer security problems that exist throughout VHA and the department. VA OIG and internal VHA reviews, along with VHA consultant studies, have consistently identified serious information system control problems at other VHA facilities.

For example, in the March 2000 report on the audit of VA's consolidated financial statements for fiscal years 1999 and 1998, VA's OIG reported that audit tests continue to demonstrate widespread weaknesses in security management, access control, application development, system software, segregation of duties, and service continuity controls. For example, at one VHA facility 3,860 users inappropriately had the ability to obtain a password file. In addition, 90 IDs at this facility remained active even though these accounts had not been used in more than a year. In March 1999, VA's OIG also reported access, ID and password management, physical security, and service continuity control weaknesses at the Carl T. Hayden Medical Center in Phoenix, Arizona.

Similarly, internal reviews of information system security at medical facilities, which were performed by VHA's central security group, identified access control and service continuity weaknesses at VHA medical facilities. For instance, more than 65 percent (17 of 26) of the medical facilities for which information system security review reports were issued from October 1999 through March 2000 were not routinely monitoring access to sensitive files. The VHA central security group also found weak password controls at 14 of the 26 medical facilities that were reviewed. Furthermore, more than 75 percent (20 of 26) of the medical facilities reviewed needed to either develop or update their contingency plans.

A consultant study commissioned by VHA's central security group to evaluate the security of VHA networks also found widespread network security weaknesses. The consultant identified several network system software configuration and password management weaknesses that it exploited to gain unauthorized high-level access to each VISN network and more than 67 percent (97 of 145) of local VHA medical facility systems connected to the network. For example, the consultant tested 124,955 network IDs and found that 46 percent were using easily guessed passwords. In addition, almost 19 percent of these passwords appeared to be default passwords that had probably been assigned initially and never changed. Although these weaknesses would not directly affect VHA's standard financial and medical applications, which are processed on different computer systems, VHA network security weaknesses increase the risk of unauthorized access to these applications. The risks created by the network security weaknesses identified by the consultant were further compounded because network access activity was not consistently monitored. In fact, the consultant reported that network access controls were not sufficient to resist even an unskilled intruder and many network systems did not have sufficient controls to detect unauthorized access.

Perhaps the most disturbing finding of the consultant study was that the weaknesses identified represented little change from those reported in a previous study conducted from January through March 1998. Although the VHA central security group had issued guidance for the implementation of standard controls on these network systems since the consultant's initial review, the consultant reported that this guidance appeared to have been almost totally ignored.

Moreover, these significant and widespread information system control problems have a departmentwide impact. VA's OIG has been reporting since fiscal year 1997 that VA programs and financial data are vulnerable to error or fraud because of departmentwide information system security control weaknesses that could materially affect VA's Consolidated Financial Statements. VA has also recognized the seriousness of computer security problems throughout the department and has reported information security as a material weakness under FMFIA since 1998.

VA Had Not Fully Established an Integrated Computer Security Management Program

One reason that computer security weaknesses persist throughout the department is that VA had not yet fully implemented a departmentwide computer security management program. This, along with the fact that VHA had not devoted adequate resources to effectively manage computer security at its medical facilities, as discussed below, has directly contributed to VHA's continuing information system control problems.

Our study of security management best practices found that leading organizations manage their information security risks through an ongoing cycle of activities coordinated by a central focal point.[13] This management process involves (1) assessing risk to determine computer security needs, (2) developing and implementing policies and controls that meet these needs, (3) promoting awareness to ensure that risks and responsibilities are understood, and (4) instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective. At VA, such a program would integrate security management programs throughout the department, including VHA, VBA, and AAC, to ensure that effective controls were established and maintained.

In October 1999, we reported that VA had (1) established a centralized computer security management group that reported directly to the acting VA CIO and (2) developed an information security program plan that generally addresses the key elements of a comprehensive computer security management program.[14] According to the security program plan, the VA central security group would provide departmentwide policy, direction, and oversight, whereas administration and staff office security groups would be primarily responsible for the implementation and oversight of departmental policies through ISOs at VA facilities.

VA has made progress in meeting several of its security program plan milestones, which also represent the department's action plan for correcting the information system control weaknesses that led VA to designate information system security as a material weakness under FMFIA. However, although the VA central security group recognizes that it must rely on security and information technology professionals in VA's component offices to accomplish departmentwide information security

[13]GAO/AIMD-98-68, May 1998.

[14]GAO/AIMD-00-5, October 4, 1999.

program objectives, VA had not yet updated its security policy to reflect the department security program plan or developed detailed guidance to ensure that key information security areas highlighted in our October 1999 report on the status of computer security at VA are fully addressed and implemented consistently throughout the department.

In October 1999, we also reported that VA organizations had independently initiated actions to improve computer security, but that these efforts were not coordinated as part of a departmentwide program. Although VHA had not completely addressed the key elements we believe to be important for effective computer security management, it had developed certain security guidance and oversight processes that could provide VA with a starting point to expedite its efforts to establish guidance in areas, such as risk assessment, intrusion detection, and security program evaluation, for which consistency and balance across the department are essential. Although our review focused primarily on VHA computer security, other VA organizations, such as AAC and VBA, had also developed guidance that could be considered for integration into the departmentwide computer security program.

VA Had Made Progress Implementing Security Program Plan Initiatives

In October 1999, we reported that VA had developed an information security program plan that described requirements for the key elements we believe to be important for effective security program management—establishing guidance and procedures for assessing risk, implementing appropriate policies and controls, raising awareness of prevailing risks, and evaluating the effectiveness of established controls. [15] The plan also (1) defined the roles and relationships of the principle stakeholders in VA's information security program and (2) set milestones for tasks related to VA security initiatives that were developed to accomplish security program plan requirements.

VA's information security program plan includes initiatives to perform a departmentwide risk assessment, establish a departmentwide incident response capability, develop Web-based security awareness and training programs, issue VA security policies, and create a departmentwide information security Intranet site. VA also developed a security initiative to acquire and implement standard software packages that would allow VA facilities to protect computer resources, identify security incidents, and

[15] GAO/AIMD-00-5, October 4, 1999.

monitor compliance with VA security policies. Some of VA's information system security program plan milestones have already been substantially met. For example, VA contracted with a consultant to operate its departmentwide critical incident response capability, created a security Web site to benefit all VA staff and ISOs, and established a Web-based security awareness curriculum.

In June 2000, VA completed a departmentwide risk assessment that resulted in an overall risk management plan that recommends specific controls necessary to reduce vulnerabilities associated with the information security risks identified. This plan also allowed VA to confirm the importance of its original information security initiatives and adjust them as necessary. The department plans to implement most of its security initiatives by May 2001 and establish a fully operational security program by January 2003. For example, VA is in the process of acquiring a Web-based ISO training program that will address basic skills that are needed by ISOs regardless of their operational setting and plans to complete the ISO training program by December 2000. VA also plans to implement a certification and accreditation program for VA systems by January 2001.

Comprehensive Policies and Guidance Remain Important

In October 1999, we recommended that VA develop detailed departmentwide guidance and oversight processes so that important aspects of computer security programs, such as assessing risk, monitoring system and user access activity, and evaluating information system policy and control effectiveness, are fully addressed and implemented consistently throughout the department.[16] Our study of security management practices at leading organizations 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.[17] 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

[16]GAO/AIMD-00-5, October 4, 1999.

[17]GAO/AIMD-98-68, May 1998.

established consistently throughout the department, but also facilitates periodic reviews of these controls.

Since our October 1999 report, VA has focused on developing specific policies based on known weaknesses. For example, VA published a policy in January 2000 to strengthen user ID and password management controls throughout the department and developed a policy that establishes minimum security requirements for electronic connections between VA computer systems and external organizations, which has been circulated to other VA organizations for concurrence. Consequently, VA had not yet updated its overall security policy to (1) reflect fundamental requirements for managing risk, determining security needs, implementing policies and controls, promoting security awareness, and evaluating the effectiveness of VA's information security program as described in the departmentwide security program plan or (2) establish specific security roles and responsibilities for implementing these requirements throughout the department. According to the director of VA's central security group, VA has drafted an updated security policy that should be implemented within the next year.

VA had also not yet developed detailed guidance to ensure that key information security areas highlighted in our October 1999 report on the status of computer security at VA—assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls—are fully addressed and implemented consistently throughout the department. We continued to find problems in these areas at each of the VHA health care systems we visited.

- Although VA and VHA policies require facilities to perform risk assessments when significant changes are made to a facility or its computer systems or at least every 3 years, VHA medical facilities were not consistently adhering to VA policy. For example, although two of the three health care systems we visited had performed some level of risk assessment in 1999, none of the health care systems we visited were updating risk assessments when significant changes, such as updating computer hardware and adding network capabilities, occurred.
- In addition, as noted above, none of the VHA health care systems we visited had established (1) proactive network monitoring programs to promptly identify unauthorized access to VA systems or (2) procedures to regularly review attempts to access sensitive information maintained on their networks for unusual or suspicious activity. Such programs are critical for ensuring that improper access to VA systems and the

sensitive information maintained on these systems is detected in time to prevent or minimize damage.
- Furthermore, none of the VHA health care systems we visited were adequately monitoring compliance with VA security policies. Routinely reviewing passwords to monitor compliance with VA guidelines that prohibit the use of common words would have allowed these medical facilities to mitigate some of the password security exposures we found.

Thus, we are reiterating the importance of establishing detailed guidance to help correct these types of weaknesses. Our October 1999 report described provisions that should be included in such guidance. The following sections summarize these requirements.

Assessing Risk

In October 1999, we reported that it was important for organizations to define a process, which could be adapted to different organizational units, to manage risk relating to computer security on a continuing basis.[18] Our study of risk assessment practices at leading organizations identified success factors that were essential for successful risk assessment programs.[19] These practices included

- designating focal points to oversee and guide the risk assessment process and help ensure that organizationwide issues were appropriately addressed;
- defining procedures for conducting risk assessments and developing tools to facilitate and standardize the process;
- involving a mix of individuals with knowledge of business operations and technical aspects of the organization's systems and security controls;
- holding business units responsible for initiating and conducting risk assessments, as well as implementing risk reduction techniques;
- limiting the scope of individual risk assessments to particular business units, systems, facilities, or sets of operations while including provisions for considering risks shared throughout the organization; and
- documenting and maintaining risk assessment results so that managers could be held accountable for the decisions made.

[18]GAO/AIMD-00-5, October 4, 1999.

[19]*Information Security Risk Assessment: Practices of Leading Organizations: A Supplement to GAO's May 1998 Executive Guide on Information Security Management* (GAO/AIMD-00-33, November 1999).

In December 1999, VA hired a consultant to perform a departmentwide risk assessment that was completed in June 2000. Although this initial assessment was not linked to the risk assessments performed at VA facilities, VA plans to (1) establish a computer security risk management program that will be coordinated by VA's information security working group to oversee and provide guidance for managing risk throughout VA and (2) develop a risk assessment procedure that specifies a process for determining and mitigating information security risks. In addition, the director of VA's central security group told us that the certification and accreditation process, which VA plans to put in place by January 2001, should provide VA facilities with a foundation for assessing and mitigating risks when significant changes to systems occur.

Monitoring System and User Access Activity

In October 1999, we also recommended that VA develop detailed guidance for monitoring system and user access activity at VA facilities to ensure that unauthorized attempts to access sensitive information maintained by VA are detected and investigated.[20] Such a program would include (1) network monitoring to promptly identify attempts by unauthorized users to gain access to VA systems and (2) examining attempts to access sensitive information once entry to VA systems is accomplished.

Guidance for establishing proactive network monitoring programs throughout VA would include provisions for

- identifying 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
- setting up an intrusion detection system to automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

Likewise, VA efforts to review access to sensitive information maintained on VA systems would be enhanced by guidance for (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

[20]GAO/AIMD-00-5, October 4, 1999.

to identify and report on access patterns that differ significantly from defined normal patterns.

In November 1999, VA established a departmentwide critical incident response capability (VA-CIRC) to improve its response to incidents, such as external or internal attacks, and to collect data for program evaluation. To support this effort, the department issued VA-CIRC operating guidelines and procedures in May 2000. However, this guidance focuses on reporting and responding to security incidents. Although this guidance contains a partial list of events that could indicate security incidents, the VA-CIRC program will not be effective until VA facilities establish programs to monitor system and user activity to identify computer security incidents. In this regard, VA's risk management plan recommended that VA implement intrusion detection software on VA networks to detect misuse by authorized users and attacks by hackers. VA also plans to establish an active monitoring mechanism to continually monitor audit logs and report unusual or suspicious access activity.

Evaluating the Effectiveness of Information System Controls

Finally, our October 1999 report stressed the importance of (1) establishing processes, such as periodic self-assessments and independent security reviews, for monitoring compliance with established security policies and guidelines, (2) directly testing information system controls to determine if risk reduction techniques that had been agreed to were, in fact, operating effectively, and (3) using the results of these efforts to improve the security program.[21] In this regard, developing technical security standards would provide VA with a basis for evaluating compliance with security policies.

At VA, such a program would include efforts at the department, administration, and facility levels. For example, individual facilities may be in the best position to periodically review user access authority for compliance with VA policy and evaluate the implementation of technical security standards; whereas independent security reviews or direct testing of certain information system controls may be more efficiently conducted at the administration or department level.

Although monitoring and testing information system controls may encourage compliance with security policies, the full benefits of these actions are not achieved unless results are used to improve the security program. Although VA had begun tracking security weaknesses, it had not

[21]GAO/AIMD-00-5, October 4, 1999.

yet developed processes to (1) independently verify that corrective actions were effectively implemented or (2) routinely analyze the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve the security environment. For example, VHA triennial reviews of information system security have consistently found that medical facilities need to either develop or update risk assessments, which would indicate that additional guidance regarding events that should trigger risk assessments may be needed.

The director of VA's central security group told us in June 2000 that the department's initial focus was on developing VA program requirements for the other critical security program management areas—assessing risk, implementing policies and controls, and promoting awareness—and collecting information on security weaknesses and incidents that would provide VA a basis for beginning to measure compliance and improving its computer security program. The director of VA's central security group also stated that the department planned on having adequate policies and processes in place by December 2000 to begin establishing an evaluation program.

VA Has an Opportunity to Build on Existing Computer Security Initiatives

In October 1999, we reported that VA organizations had independently acted to improve computer security, but that these efforts were not coordinated as part of a departmentwide program.[22] Our review focused on security management within VHA, which—like other VA organizations—had developed certain security guidance and oversight processes relating to the key security management areas we highlighted in our October 1999 report on the status of computer security at VA. Even though VHA security management policies and procedures did not fully address the critical elements we believe to be important for effective computer security management, they—along with security guidance and processes established by other VA organizations—could provide VA a starting point to expedite the development of overall departmental policies and procedures for assessing risk, monitoring access activity, and evaluating the effectiveness of information system controls.

VA had established a computer security working group with representatives from the VA central security group and all VA line and staff organization security groups, and the VA central security group

[22]GAO/AIMD-00-5, October 4, 1999.

participated in VHA's review process for security policy and guidance. However, the department had not yet integrated the efforts of other VA organizations into the overall departmentwide program. For example, VHA had drafted, but not yet issued, guidance for assessing risk throughout VHA that addressed several practices that we identified as critical to successful risk assessment programs. The draft VHA risk assessment framework included provisions for holding business units responsible for performing and acting on risk assessments, limiting the scope of individual risk assessments, and documenting and maintaining the results of risk assessments. In addition, VHA had developed a risk assessment guideline that established a process, along with a sample memo, for documenting risks identified, possible consequences associated with the risks identified, recommendations for addressing risks identified, and the facility director's decision to address or accept the risks identified.

We also reported in June 1999[23] that AAC had begun reviewing failed attempts to access sensitive data and resources and planned to expand its monitoring efforts to identify and investigate unusual or suspicious patterns of access to sensitive resources, such as changes to sensitive system files that were not performed by system programmers and revisions to production data that were completed by system or application programmers. In addition, VHA had drafted an incident response guideline that includes sections on protecting computer systems from and identifying certain types of security incidents, such as computer viruses and attempts by unauthorized individuals to gain access to VA systems. Furthermore, although VA had recently issued technical security standards for the network, AAC and VHA had developed technical security standards for other common VA operating environments.

Other organizations had also established processes that could be incorporated into a departmentwide program for evaluating the effectiveness of information system controls. As we reported in October 1999, both VBA and VHA had developed information security self-assessment tools. In addition, VHA's central security group performs triennial reviews of information security at VHA facilities. Moreover, VHA had commissioned studies to test network security within VHA that could be expanded to evaluate computer security throughout the department.

[23] *VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls* (GAO/AIMD-99-161, June 8, 1999).

These examples of computer security guidance and processes illustrate the types of security activities that could be considered for integration into the departmentwide computer security program. Initiating a process to review and build on existing security practices developed by different VA organizations into the departmentwide program could expedite VA efforts to develop departmentwide guidance for assessing risk, monitoring system and user access activity, and evaluating information system controls. Such a process would also help ensure that security resources are expended efficiently and increase consistency in implementing security procedures because different VA organizations could adapt departmentwide guidance to meet their organizational needs as opposed to developing such guidance independently.

Adequate VHA Computer Security Management Resources Are Essential

In October 1999, we reported that the ultimate success of VA's computer security management program depended 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.[24] In 1999, VA developed an information security budget plan that depends on both departmental and administration resources to accomplish departmentwide security initiatives. The VA Capital Investment Board approved the security program budget plan for fiscal years 2000 through 2005. In addition, VA's information security program called for an initial investment at the end of fiscal year 1999 for which VA's CIO Council established an apportionment formula based on the number of employees at VA's three administrations and the Office of Information and Technology. All of these organizations contributed their portion of the fiscal year 1999 funds and, according to the director of VA's central security group, most VA components continued to demonstrate their commitment by contributing fiscal year 2000 funds. However, VHA, which was expected to contribute more than 90 percent of VA's central security program budget requirements for fiscal year 2000, had not yet complied. Consequently, VA's ability to continue to develop and implement its departmentwide computer security management program is in jeopardy. For example, VA initiatives to strengthen information system controls by implementing standard security products throughout the department cannot be accomplished unless VA can rely on VHA's expected contributions. Moreover, most VHA medical facility directors had not yet

[24]GAO/AIMD-00-5, October 4, 1999.

committed sufficient security oversight resources to substantially improve computer security at individual medical facilities.

Security Oversight Had Not Been Adequately Addressed at Medical Facilities

In addition to funding the departmentwide security program, it is important for VHA to ensure that its central security group and medical facilities have adequate resources to implement security program requirements effectively. Although VHA had established a central security group within the CIO's organization to establish and oversee computer security throughout the administration, the director of each medical facility is responsible for implementing and monitoring the facility's information security program through a designated ISO. As such, VHA ISOs are responsible for developing and implementing facility information security policies and procedures that establish security management, operational, and technical controls described in the VHA security policy; making sure that risk analysis and certification and accreditation procedures have been performed and documented along with contingency plans and rules of behavior in system security plans for each facility computer system; providing security training for facility staff; and ensuring that the facility information security policies and procedures are adhered to.

Placing the responsibility for developing, implementing, and overseeing facility information security programs at this level is appropriate because individual units are most familiar with the sensitivity and criticality of their data and have the most to lose if poor security negatively affects their operations. However, the medical facility directors responsible for implementing VHA's computer security program had not taken steps to ensure that the facility ISO positions were adequately staffed. Consequently, VHA medical facilities were not managing computer security well. For example, as we noted above, VHA facilities had not made much progress in addressing weaknesses identified by a consultant study despite the fact that the VHA central security group had developed guidance for implementing controls that would have corrected these weaknesses.

Although the three health care systems that we visited had recently recognized the lack of attention given to computer security at their facilities and committed to making the ISO a full-time position, computer security had not received adequate attention at most other medical facilities. At more than 85 percent of the 149 medical facilities for which information was available, directors had assigned information security as a collateral responsibility. In addition, half of the 22 VISNs did not have a full-time ISO in their entire organization—either at the VISN or medical facility

level. According to a 1999 survey conducted by VHA's central security group, more than half of the ISOs that responded devoted about 15 percent of their time to security-related matters, which was not sufficient to actively manage and monitor access to critical medical and financial systems. In addition, these security staff served in diverse and unrelated occupations—such as police chief, nurse, audiologist, dietician, and social worker—suggesting that many of the ISOs may not be technically qualified to implement and monitor facility computer security programs. Also, about 30 percent of the ISOs at the 149 medical facilities for which information was available had been assigned to the position for less than 2 years, further compounding the lack of consistent focus on computer security at the facility level.

In March 2000, VHA's central security group issued a policy requiring (1) a full-time ISO at larger and consolidated facilities and (2) ISO duties to be assigned as a primary responsibility at smaller facilities. Adherence to this policy should greatly improve the effectiveness of computer security management at each of the medical facilities affected by this policy. To support facility efforts to improve security oversight, VHA's central security group was in the process of clearly defining ISO roles and responsibilities. According to the director of VHA's central security group, his staff planned to publish specific ISO roles and responsibilities as a VHA security guideline and distribute a brochure outlining recommended ISO skill sets by September 2000.

Recognizing that most ISOs do not have information systems backgrounds, both the department and VHA central security groups plan to establish ISO training programs. VA plans to establish a Web-based ISO training program to address basic skills that are needed by ISOs regardless of their operational setting by December 2000. In addition, the VHA central security group, in conjunction with VHA's National Training and Education Office, had implemented an ISO training program specific to VHA that would provide ISOs with a basic understanding of security management, operational, and technical controls required to secure VHA resources.

Conclusions

Access control and service continuity problems are placing financial and sensitive veteran medical information at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and/or destruction. While the health care systems we visited had corrected most of the specific computer security weaknesses we identified in 1998, we found additional access control and service continuity problems at these facilities and serious

weaknesses at the VA Maryland Health Care System. Similar security problems also persist throughout VHA and the department.

One reason for VA's continuing information system control problems is that it had not established an effective, integrated computer security management program throughout the department. VA had made progress in implementing its plan to improve computer security throughout the department. Even so, it remains important for VA to develop detailed guidance to ensure that the key program elements we highlighted in our October 1999 report[25]—periodically assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls—are fully addressed and implemented consistently across the department. Consequently, we are reaffirming our October 1999 recommendation for VA to develop detailed guidance in these areas. To expedite departmental efforts to establish such guidance, VA could incorporate and build upon guidance and processes developed by other VA organizations.

Moreover, VA's ability to continue to develop and implement an effective computer security management program is in jeopardy because VHA had not yet (1) contributed its portion of the funds required to support fiscal year 2000 departmentwide security initiatives or (2) devoted adequate resources to security oversight at medical facilities.

Recommendations

We recommend that the Acting Secretary of Veterans Affairs direct the acting VA CIO to work with the VHA CIO and medical facility directors as appropriate to

- ensure that the remaining computer security weaknesses at each health care system we visited, which are summarized in appendix II, are corrected in accordance with the action plans developed by each of the medical facilities and detailed in our separate reports to the facility directors and
- provide security oversight resources as prescribed in VHA policy to effectively implement and oversee VA's computer security management program through assessing risk, implementing policies and controls,

[25]GAO/AIMD-00-5, October 4, 1999.

promoting awareness, and evaluating the effectiveness of information system controls at VHA facilities.

In addition, to facilitate the development of detailed departmentwide guidance and oversight processes relating to key aspects of computer security programs, such as assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls, as we recommended in October 1999 and reaffirmed in our conclusions above, we recommend that the Acting Secretary of Veterans Affairs direct the acting VA CIO to implement a cooperative process across all VA component offices that would identify and, where appropriate, integrate security guidance developed by VA components.

We also recommend that the Acting Secretary of Veterans Affairs direct the acting VA CIO to monitor and report to you for resolution, issues, such as an administration's lack of commitment of resources to the departmentwide program, that could affect the development and implementation of VA's departmentwide computer security program.

Agency Comments

In commenting on a draft of this report, VA agreed with our recommendations and stated that it intends to develop an accelerated plan to improve information security at its facilities. Specifically, VA stated that it would track the resolution of the recommendations we made to correct specific information security weaknesses at the health care systems we visited. In addition, VA provided examples of security management activities performed by the VHA central security group to implement and oversee computer security throughout the administration. However, to fully address our recommendations, VA will need to provide adequate security oversight resources at each of its VHA facilities to implement security program requirements at these facilities.

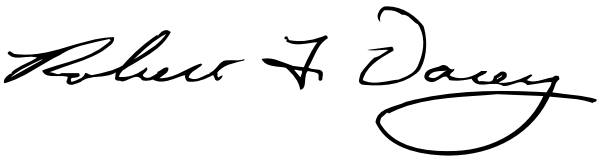
VA also stated that it would use its Information Security Working Group, which includes representatives from all administration and staff office security groups, to develop departmentwide policy, guidance, and processes. This approach could provide VA the opportunity to identify and, where appropriate, integrate security guidance and oversight processes developed by VA components into the departmentwide program. Finally, VA stated that it has implemented several management reporting processes to ensure that security program issues, particularly those of a financial nature, are addressed.

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 more than 60 days after the date of this report.

We are sending copies of this report to Senator Robert C. Byrd, Senator Joseph Lieberman, Senator John D. Rockefeller IV, Senator Arlen Specter, Senator Ted Stevens, Senator Fred Thompson, Representative Dan Burton, Representative Lane Evans, III, Representative David Obey, Representative Bob Stump, Representative Henry A. Waxman, and Representative C. W. (Bill) Young 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 report are listed in appendix III.

Sincerely yours,



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

Comments From the Department of Veterans Affairs

Note: GAO's comment supplementing those in the report text appears at the end of this appendix.

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

AUG 17 2000

Mr. Jeffrey C. Steinhoff
Assistant Comptroller General
Accounting and Information Management Division
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20420

Dear Mr. Steinhoff:

We have reviewed your draft report, ***VA INFORMATION SYSTEMS: Computer Security Weaknesses Persist at the Veterans Health Administration*** (GAO/AIMD-00-232) and concur in your recommendations.

I am indeed concerned with these information system security control deficiencies that GAO has identified in the Department of Veterans Affairs. While they are common to all Federal agencies, I am dissatisfied with the pace of their resolution in VA. Therefore, I am instructing the acting CIO to develop an accelerated plan to upgrade information security controls at the Department's field facilities as well as VA Central Office.

The enclosure addresses your recommendations in detail. I appreciate the opportunity to comment on your draft report.

Sincerely,

Hershel W. Gober
Acting

Enclosure

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
COMMENTS TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Security Weaknesses Persist at the Veterans Health Administration
(GAO/AIMD-00-232)

GAO recommends that I direct the acting VA CIO to work with the VHA CIO and medical facility directors as appropriate to:

- **ensure that the remaining computer security weaknesses at each health care system we visited, which are summarized in Appendix I, are corrected in accordance with the action plans developed by each of the medical facilities and detailed in our separate reports to the facility directors;**

Concur - VHA is already using its established followup process to track completion of the recommendations at each of the health care systems visited through its Office of Policy and Planning, Management Review and Administration Service's Electronic Record Management Information System (ERMIS).

- **provide security oversight resources as prescribed in VHA policy to effectively implement and oversee VA's computer security management program through assessing risk, implementing policies and controls, promoting awareness, and evaluating the effectiveness of information system controls at VHA facilities.**

Concur - VHA has in place policy and controls. The Medical Information Security Service on a triennial basis reviews these, and action plans addressing vulnerabilities are provided to each facility. A security risk assessment for VHA components is due for completion in August 2000, which may recommend changes to alter/enhance current policy and controls in recognition of the changing IT environment. VHA continues to provide awareness activities, including on-line courses for Information Security Officers and Information Resources Management staff, and developing brochures, pamphlets and posters. In addition, VHA conducts an annual information security conference, which has seen an increase in attendance over the past four years of 30 percent. VHA also provides and manages a virus protection program which, beginning this year, will allow us to monitor the effectiveness of the distribution of this product to currently over 150,000 nodes.

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
COMMENTS TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Security Weaknesses Persist at the Veterans Health Administration
(GAO/AIMD-00-232)
(Continued)

In addition, to facilitate the development of detailed departmentwide guidance and oversight processes relating to key aspects of computer security programs, such as assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls, as we recommended in October 1999 and reaffirmed in our conclusions above, we recommend that the Secretary of Veterans Affairs direct the acting VA CIO to work with administration CIOs and facility directors as appropriate to establish a process for identifying, reviewing, and integrating security guidance and oversight processes developed by other VA organizations into the departmentwide program;

See comment 1.

Coordination between GAO and VA staffs has resulted in the following language to be substituted:

"... we recommend that the Acting Secretary of Veterans Affairs direct the Acting CIO to implement a cooperative process across all VA component offices that would identify and, where appropriate, integrate security guidance developed by VA components.

Concur - VA's Departmental Information Security Working Group collaborates to develop Departmentwide policy, guidance, and processes. This Working Group is comprised of all Administration and staff office security management offices. The Working Group operates under the guidance, and reports to, VA's CIO Council. Policies that are proposed for issuance Departmentwide are submitted to the CIO Council for approval, and are processed through VA's formal Directives Management System. These management controls assure that Departmentwide security policies, procedures, and processes are thoroughly and equitably vetted.

We also recommend that you direct the acting VA CIO to monitor and report issues that could affect the development and implementation of VA's departmentwide computer security program, such as an administration's lack of commitment of resources to the departmentwide program, to you for resolution.

Concur - VA has several management reporting processes in place to assure that security program issues, in particular those of a financial nature, are addressed. Principally, these processes include the capital investment execution review process, the VA Resources Board quarterly budget reviews, FMFIA Material Weakness Program

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
COMMENTS TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Security Weaknesses Persist at the Veterans Health Administration
(GAO/AIMD-00-232)
(Continued)

reviews, and the monthly meetings of VA's CIO Council. We are confident that the budget basis for the Department program is now settled because beginning FY 2001 VA has a funded capital investment plan for the program.

VHA has designated FY 2000 funds of over $2 million to support initiatives already approved by the Capital Investment Board in support of the Department Security Initiative. Those funds will be released following approval by the VHA Information Technology Advisory Board, the Screening and Evaluation Committee and the Policy Board. Discussion continues to resolve issues of scope, cost estimates of VHA's portion of the $17.5 million needed to fund the complete initiative and how to leverage ongoing VHA activities in this area.

The following is GAO's comment on the Department of Veterans Affairs' letter dated August 17, 2000.

GAO Comment

Based on discussions with VA management officials, we made some wording changes to this recommendation. However, the essence of our recommendation has not changed.

Computer Security Weaknesses We Identified at Three VHA Health Care Systems

This appendix summarizes the information system control weaknesses we identified during our work at the VA Maryland Health Care System (VAMHCS), the New Mexico VA Health Care System (NMVAHCS), and the VA North Texas Health Care System (VANTHCS) that remained open at the completion of our 1999 site visits. These weaknesses are grouped based on the type of controls identified in our *Federal Information System Controls Audit Manual*, which provides guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data associated with federal agency operations.

Computer security weakness	Affected health care system
Network access controls	
System settings could permit individuals to establish connections without entering valid user account name and password combinations (authentication).	VANTHCS NMVAHCS VAMHCS
A parameter that controls a system service was not configured to effectively prevent unauthorized access to a network system.	VANTHCS
Certain network system software had not been updated to reflect the most recent vendor upgrades.	VANTHCS
On one network system used to provide system access from remote locations, an optional system parameter that allowed the system to automatically log on to an administrator account without user interaction had been enabled.	VANTHCS
All users were granted access that allowed the creation and deletion of files and subdirectories in sensitive system directories.	NMVAHCS VAMHCS
Warning banners were not displayed on the initial logon screen.	NMVAHCS VAMHCS
Passwords associated with a network router, including the powerful administrator password, were not encrypted.	NMVAHCS
Network ID and password management controls	
Generic user IDs were being shared.	VANTHCS VAMHCS
Network passwords were common words or characters that could be easily guessed or identified through commonly available hacker tools.	VANTHCS NMVAHCS VAMHCS
Passwords were not periodically reviewed to ensure compliance with VA password guidelines.	VANTHCS NMVAHCS VAMHCS
Network passwords were set to the default password or a slight variation of the default password assigned when the ID was created.	VANTHCS NMVAHCS
Network passwords were set to never expire.	VANTHCS NMVAHCS VAMHCS

(Continued From Previous Page)

Computer security weakness	Affected health care system
Minimum network password length was less than six characters.	NMVAHCS VAMHCS
Network system settings allowed unlimited logon attempts.	VAMHCS
A network file accessible to all users contained passwords that were stored in clear text.	VAMHCS
IDs belonging to terminated or transferred employees were not promptly deactivated.	VANTHCS NMVAHCS VAMHCS
Inactive network IDs were not disabled promptly.	VANTHCS NMVAHCS VAMHCS
Remote access controls	
Remote access control policies and procedures had not been established.	VANTHCS NMVAHCS VAMHCS
Network security monitoring	
Proactive network monitoring programs to identify unusual or suspicious activities had not been implemented.	VANTHCS NMVAHCS VAMHCS
Information system control policies did not require procedures for event logging and maintaining audit trails of access activities that would warrant review. Although some network activities were logged, these logs were not reviewed regularly. In addition, when audit logs were reviewed, the reviews were not documented to show the results of the review.	VANTHCS NMVAHCS VAMHCS
Network intrusion detection capabilities were not activated on at least one network server.	NMVAHC
User access controls	
Procedures to ensure that IDs with access to all medical and financial data were adequately controlled had not been established.	VANTHCS NMVAHCS VAMHCS
A powerful user ID (postmaster) was shared by 15 staff, even though these staff members had individual accounts.	NMVAHCS
Procedures for granting access to users were not being followed.	NMVAHCS VAMHCS
Segregation of duties	
The security officer reports to the director of Information Resource Management (IRM), which may impair the security officer's independence when assessing security within the IRM function.	VANTHCS
Staff involved with procurement had the ability to request, approve, and receive medical items without management approval, which violates basic segregation of duties principles and VA policy.	NMVAHCS VAMHCS
Application development and change control	
Procedures for periodically reviewing modifications to standard VHA application programs had not been established to ensure that only authorized program code was implemented.	NMVAHCS VAMHCS
Service continuity	
Service continuity plans were not complete.	VANTHCS VAMHCS
Annual testing of the service continuity plan, as required by VA and VHA policy, had not been performed.	VANTHCS

(Continued From Previous Page)

Computer security weakness	Affected health care system
Periodic walk-throughs and unannounced tests of service continuity plans were not performed.	NMVAHCS VAMHCS
Critical backup files for financial and sensitive veteran medical programs, data, and software were not stored off-site.	NMVAHCS
Physical security controls	
Sensitive telecommunication cables and wiring panels were not adequately protected to prevent disruptions to computer operations.	VANTHCS
Formal procedures for granting access to the computer room based on job responsibilities had not been developed.	VANTHCS NMVAHCS VAMHCS
Procedures for periodically accounting for all keys to the computer room had not been established.	NMVAHCS VAMHCS
Access to critical computer support facilities was not adequately secured.	VAMHCS
Combustible materials were stored in the wiring closets.	NMVAHCS
Computer security management	
A risk assessment of all major systems had not been performed within the last 3 years.	VAMHCS
Risk assessment documentation did not address actions taken to mitigate risks identified.	VANTHCS NMVAHCS
A process had not been established to assess risk when significant changes to computer systems occurred.	VANTHCS NMVAHCS VAMHCS
A structured security training curriculum had not been developed.	NMVAHCS
Information security officers performed security oversight as a collateral duty and had not received security training in center systems.	NMVAHCS VAMHCS
A program to routinely evaluate the effectiveness of information system controls had not been established.	VANTHCS NMVAHCS VAMHCS
A formal incident response plan and an associated team had not been implemented to ensure efficient and timely responses to information system security incidents.	VAMHCS

GAO Contact and Staff Acknowledgements

GAO Contact

Dave Irvin, (214) 777-5716

Acknowledgements

In addition to the person named above, Lon Chin, Debra Conner, Shannon Cross, Denise Fitzpatrick, Jeffrey Knott, Harold Lewis, Norman Poage, Charles Vrabel, and Christopher Warweg made key contributions to this report.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. 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

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

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
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.

Orders by Internet:
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

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

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