



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284614

March 24, 2000

Mr. Norman E. Browne
Chief Executive Officer, New Mexico VA Health Care System
Department of Veterans Affairs
1501 San Pedro Drive, SE
Albuquerque, New Mexico 87108

Subject: VA Systems Security: Information System Controls at the
New Mexico VA Health Care System

Dear Mr. Browne:

As part of our review of computer security at the Department of Veterans Affairs (VA), we assessed the effectiveness of information system general controls¹ at the New Mexico VA Health Care System (NMVAHCS). Our review of VA computer security was performed in connection with the department's required annual financial statement audit for fiscal year 1999. Our evaluation included a follow-up on the computer security weaknesses we identified at NMVAHCS in conjunction with the audit of VA's fiscal year 1997 financial statements.²

The purpose of this report is to advise you of the weaknesses we identified at NMVAHCS and the status of corrective actions. In discussions with your staff, we offered specific recommendations for mitigating these weaknesses. The results of our evaluation will be shared with VA's Office of Inspector General for its use in auditing VA's consolidated financial statements for fiscal year 1999.

In evaluating information system general controls, we identified and reviewed NMVAHCS's information system control policies and procedures. We also tested and observed the operation of information system general controls over NMVAHCS's

¹General 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*Information Systems: VA Computer Control Weaknesses Increase the Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 23, 1998).

financial systems to determine whether they were in place, adequately designed, and operating effectively. These controls, however, also affect the security and reliability of nonfinancial information, such as the medical support systems maintained at this center. Our evaluation of information system general controls was based on our *Federal Information System Controls Audit Manual (FISCAM)*,³ which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data associated with federal agency operations.

In addition, we determined the status of previously identified information system general control weaknesses. We discussed the status of corrective actions with NMVAHCS officials. Where those officials indicated that corrective actions had been taken, we observed and tested the controls placed into operation to assess their effectiveness.

NMVAHCS made progress in correcting specific computer security weaknesses that we identified in our previous evaluation of information system general controls. NMVAHCS had resolved 15 of our prior recommended actions. For example, NMVAHCS had reduced the number of users with certain powerful system privileges and limited access to the computer room to those users who needed it to carry out their assigned responsibilities. In addition, NMVAHCS was conducting tests of its disaster recovery plan, maintaining copies of the plan off-site, and periodically reviewing the plan to keep it current.

However, we identified significant weaknesses that pose a risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and destruction of financial and sensitive veteran medical information. Of particular concern was NMVAHCS's lack of adherence to the internal control standard on segregation of duties, which prescribes that key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. Specifically, we identified 11 staff involved with procurement that had system access privileges that allowed them to individually request, approve, and record the receipt of medical items purchased. In addition, 9 of the 11 staff had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about \$300,000, that were requested, approved, and receipt recorded by the same individual. These purchases were made by 6 of the 11 staff with system access privileges. VA policy requires that purchases that are requested, approved, and received by the same individual have VA management approval. We found no evidence of this approval, nor did NMVAHCS have mitigating controls in place to alert management of purchases made in this manner.

When staff control all key aspects of a process, as described above, it increases the risk that unauthorized, and even fraudulent, transactions may occur. At the completion of our fieldwork, your staff were reviewing these purchases to ensure

³*Federal Information System Controls Audit Manual, Volume I – Financial Statement Audits* (GAO/AIMD-12.19.6, January 1999).

their appropriateness. In February 2000, NMVAHCS officials told us that they had reviewed the 60 purchases and found no evidence of fraud or abuse. In addition, NMVAHCS officials stated that they had developed a software program for management purposes to audit and report on these types of purchase activities monthly.

In addition, we found that NMVAHCS had not (1) established effective access controls to its network and main computer system, (2) adequately managed network user identifications (ID) and passwords, or (3) monitored network system activity. Moreover, NMVAHCS had not established comprehensive physical security controls or implemented all key components of a comprehensive service continuity plan. In all, our work identified 28 specific open weaknesses.

The lack of a comprehensive computer security management program is the primary reason for NMVAHCS' continuing information system general control problems. Our May 1998 study of security management best practices⁴ found that an effective program would include guidance and procedures for assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. While NMVAHCS was completing a risk assessment during our site visit, the center did not have a process for assessing risks when enhancements are made to its computer environment, such as the recent implementation of its Windows NT network. Furthermore, it had not established a framework to include all other key elements of a successful computer security management program, as described above.

We are recommending actions to correct each of the 28 individual computer security weaknesses that remained open at the completion of our site visit. Enclosure 1 describes these weaknesses in more detail and offers specific recommendations to resolve each of them. While some of the network access control weaknesses cannot be corrected without specific efforts by the Veterans Integrated Service Network (VISN) and VA national office, NMVAHCS needs to continue to work with these offices to ensure resolution of these weaknesses. Enclosure 2 summarizes the computer control weaknesses that NMVAHCS corrected.

In January 2000, NMVAHCS provided us with a corrective action plan to address the remaining open weaknesses we identified during this review. Proper implementation of this plan should correct all previously identified security issues and ensure that an effective computer security environment is achieved and maintained. The plan included updated information regarding corrective actions taken since we completed our fieldwork. We did not verify that these corrective actions had been implemented but plan to do so as part of future reviews.

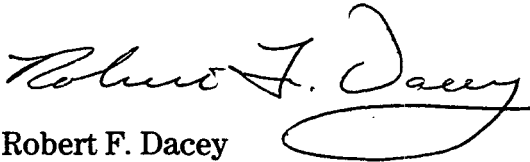
We performed our review at NMVAHCS from November 1999 through January 2000, in accordance with generally accepted government auditing standards. We requested

⁴*Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

comments from you on a draft of this letter. On March 7, 2000, you and your executive office staff told us that you agreed with our findings and recommendations. You stated that in many cases, NMVAHCS has subsequently corrected many of the reported computer security vulnerabilities and has a corrective action plan to resolve the remaining open weaknesses by October 2000. In addition, you told us that you have recently approved the establishment of a full-time information security officer position to enhance your overall computer security program. Further, you stated that while NMVAHCS will be working with the VISN and VA national office to correct some of the weaknesses identified, the ultimate ability to correct these weaknesses rests with these offices.

We are sending a copy of this letter to Harold Gracey, Principal Deputy Assistant Secretary for Information and Technology, Department of Veterans Affairs; Charles Yarbrough, Acting Chief Information Officer, Veterans Health Administration; and Richard Griffin, Inspector General, Department of Veterans Affairs. If you have any questions or wish to discuss this report, please contact me at (202) 512-3317. Other contacts and key contributors to this letter are listed in enclosure 3.

Sincerely yours,

A handwritten signature in cursive script that reads "Robert F. Dacey". The signature is written in dark ink and is positioned to the left of the printed name.

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

Enclosures

**Computer Security Weaknesses at NMVAHCS
That Remain Open**

This enclosure summarizes the information system control weaknesses we identified during our work at NMVAHCS during 1997 and 1999 that remained open at the completion of our most recent site visit. For each weakness, the enclosure provides recommended actions and management's response. These weaknesses are grouped based on type of controls identified in our FISCAM. The year that the control issue was identified is included in parentheses after the description of each weakness.

Network Access Controls

A basic management objective for any organization is to protect its data from unauthorized access and prevent improper modification, disclosure, or deletion of financial and sensitive information. To reduce the risk of unauthorized access, organizations need to sufficiently protect access to their network. Because of VA's highly interconnected environment, the failure to control access to any one system connected to the network exposes all systems and applications attached to the network even if each of the remaining NMVAHCS systems have ample security. As a result, financial information and sensitive veteran's medical information could be at increased risk of unauthorized modification or disclosure occurring without detection. At NMVAHCS, we identified, for example, the following security weaknesses.

1. **Weakness:** System settings on one of the network servers could permit individuals to establish connection without entering a valid user account name and password combination (authentication). Through this connection, an unauthorized individual could gain access to information contained in the system that would allow the individual to understand the network environment, including user account names, password properties, and account policy details, and target administrative users with password-cracking software. (1999)

Recommendation: Change system settings to prohibit individuals from gaining unauthorized access to system information.

Management Response: In January 2000, NMVAHCS officials told us that they are working with VISN and VA national office, which have the responsibility for changing network system settings. They expect this issue to be corrected by October 2000.

2. **Weakness:** Excessive user rights were granted on one of the network systems, which could compromise the integrity of the operating system. For example, all 1,100 users were granted access to sensitive system directories that would allow users to create files and subdirectories and delete files and subdirectories or the current directory. Also, all users had access to certain system settings that would allow them to create or set system parameters that could execute malicious code upon system start-up. (1999)

Recommendation: Restrict access to sensitive system directories and files to those individuals who need such access to perform their duties.

Management Response: In January 2000, NMVAHCS officials told us that they are working with VISN and VA national office, which have the responsibility for changing network system settings. They expect this issue to be corrected by October 2000.

3. **Weakness:** The network system was not set to display a warning banner on the initial log-on screen. As a result, NMVAHCS may be unable to prosecute or take disciplinary action against individuals who misuse its system. (1997)

Recommendation: Create a warning banner to be displayed on the initial log-on screen.

Management Response: In January 2000, NMVAHCS officials told us that they are working with VISN and VA national office, which have the responsibility for changing network system settings. They expect this issue to be corrected by October 2000.

4. **Weakness:** Passwords associated with the network router, including the powerful administrator password, were not encrypted. This increases the possibility that the router password could be easily identified, allowing an unauthorized user the capability to modify access rules, system audit logs, and other security parameters. (1999)

Recommendation: Change router settings to encrypt passwords.

Management Response: In January 2000, NMVAHCS officials told us that they are working with VISN and VA national office, which have the responsibility for changing network system settings. They expect this issue to be corrected by October 2000.

Network ID and Password Management Controls

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 contain specified numbers and types of characters, and not common words; and default IDs and passwords are changed to prevent their use.

In addition, we found several areas where NMVAHCS was not adequately controlling IDs and passwords as described below.

5. **Weakness:** About 90 percent of 1,100 network IDs, including user IDs that had special privileges, were vulnerable to abuse because passwords were common words or characters that could be easily guessed. NMVAHCS was not reviewing passwords to ensure compliance with VA password guidelines. (1999)

Recommendation: Increase employee awareness of VA's password guidelines, and periodically review passwords to ensure compliance with those guidelines.

Management Response: In January 2000, NMVAHCS officials told us that they plan to (1) implement a program to increase employee awareness of VA's password guidelines and (2) periodically review passwords to ensure compliance with the guidelines. NMVAHCS officials expect to complete this action by September 2000.

6. **Weakness:** About 195 network users continue to use the default password provided when the account was created. This increases the risk that commonly known passwords could be used to obtain improper access to the NMVAHCS system. (1999)

Recommendation: Increase employee awareness about the importance of not continuing to use default passwords and periodically review passwords to ensure that default passwords are not being used.

Management Response: In January 2000, NMVAHCS officials told us that they would implement a program to increase employee awareness about the importance of not continuing to use default passwords and periodically review passwords to ensure that default passwords are not being used. NMVAHCS officials expect to complete this action by September 2000.

7. **Weakness:** Four user accounts with special privileges had passwords that were set to never expire. Since the password setting established for individual user accounts takes precedence over the systemwide maximum password age parameter, these users never have to change their password. Consequently, there is greater risk for these passwords to be compromised, potentially leading to unauthorized use of passwords and user accounts to gain access to system resources. (1999)

Recommendation: Change the password settings to require passwords to periodically expire.

Management Response: In January 2000, NMVAHCS officials told us that this issue has been resolved by VISN changing the password settings for those accounts that had passwords set to never expire. System settings were also changed to prohibit nonexpiring passwords.

8. **Weakness:** On one network, system settings did not require users to change passwords after a specified period of time. By not requiring users to periodically

Enclosure 1

change their passwords, the risk becomes greater that unauthorized users could continue to use captured passwords. (1999)

Recommendation: Update system password settings to require that passwords be periodically changed.

Management Response: In January 2000, NMVAHCS officials told us that this issue has been resolved by VISN changing password settings so that users are required to periodically change their passwords.

9. **Weakness:** The minimum password length on one network was set to two characters. This allows users to use very short passwords that are easier to guess than longer passwords. (1999)

Recommendation: Change system password setting to require longer passwords.

Management Response: In January 2000, NMVAHCS officials told us that this issue has been resolved by VISN changing password settings to require passwords to be at least seven characters in length.

We also found that NMVAHCS was not promptly removing access authority for terminated or transferred employees or deleting unused or unneeded IDs.

10. **Weakness:** Fifty-nine network IDs and over 100 system IDs belonging to terminated or transferred employees were not disabled. If these IDs are not promptly disabled when employees are terminated, former employees are allowed the opportunity to sabotage or otherwise impair NMVAHCS operations. (1997)

Recommendation: Disable IDs belonging to terminated or transferred employees. Periodically review IDs to identify terminated or transferred employees and develop policies and procedures for removal of IDs for terminated or transferred employees.

Management Response: NMVAHCS officials told us that as of January 2000, policies and procedures were in place for VISN staff to provide them a list of active network users to identify IDs of terminated or transferred employees that need to be removed. Additionally, as of January 2000, a list of system users was being generated regularly for department validation.

11. **Weakness:** About 200 network IDs and 28 system IDs had not been used for over 90 days. Allowing this situation to persist poses unnecessary risk that unneeded IDs will be used to gain unauthorized access to NMVAHCS computer resources. (1997)

Recommendation: Periodically review user accounts and disable IDs that are unneeded.

Management Response: NMVAHCS officials told us that procedures are in place as of January 2000 for VISN staff to provide them a list of active network users for validation by service personnel. Additionally, by June 2000, a program will be run every week to review user accounts that have not been active for over 90 days. IDs identified in this process will be disabled.

Remote Access Controls

Organizations must control access to computer resources from remote locations to protect sensitive information from improper modification, disclosure, or destruction by hackers. Because allowing dial-in connections from remote locations significantly increases the risk of unauthorized access, such access should be limited, justified, approved, and periodically reviewed. Organizations should also control all modems and telephone lines centrally, establish controls to verify that dial-in connections are authorized, and test for unauthorized modems.

12. **Weakness:** NMVAHCS had not established remote access control policies or procedures to require that dial-in connections to internal systems and network be authorized and prohibit employees from connecting unauthorized modems to network workstations. NMVAHCS had not established formal procedures for periodically testing dial-in connections or validating users with remote access privileges to ensure that those connections and privileges were authorized and appropriate. (1999)

Recommendation: Establish and implement policies and procedures to authorize and review dial-in connections.

Management Response: In January 2000, NMVAHCS officials told us that a policy and procedure for modem and remote access connections was being drafted and should be completed by June 2000. This policy will provide guidance on the authorization, configuration, and monitoring of modem use.

Network Security Monitoring

To reduce the risks created by network access control problems, organizations need to establish proactive network monitoring programs. These programs require organizations to promptly identify and investigate unusual or suspicious network activity indicative of malicious, unauthorized, or improper activity, such as repeated failed 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. Network monitoring programs should also include provisions for logging and regularly reviewing network access activities. Without such controls, organizations have little assurance that unauthorized access to systems on their network would be detected in time to prevent or minimize damage.

13. **Weakness:** NMVAHCS did not have a proactive network-monitoring program to identify unusual or suspicious activities. Moreover, NMVAHCS did not have a

policy that required procedures for logging system events and maintaining audit trails of access activities that would warrant further review. Although NMVAHCS was logging some of its network activities, these logs were not reviewed regularly and, for those that had been reviewed, NMVAHCS had not retained documentation showing the results of its review. Such reviews should be done routinely to track and analyze activities that could be indicative of unusual or suspicious activities. (1997)

Recommendation: Establish a proactive network monitoring program to identify unusual or suspicious activities.

Management Response: In January 2000, NMVAHCS officials told us that they were working with VISN to establish a proactive network monitoring program that will include implementing procedures for logging system events and maintaining audit trails of access activities. NMVAHCS officials expect this action to be completed by October 2000.

14. **Weakness:** NMVAHCS did not have its network intrusion detection capabilities activated on at least one of the Novell servers. Without this feature being active, NMVAHCS would not receive any notification of an unauthorized user making unlimited attempts to gain access to special user accounts, including administrative accounts. Gaining such privileges would allow unauthorized users to have access to all system resources. (1999)

Recommendation: Activate network intrusion detection capabilities on the server.

Management Response: NMVAHCS officials told us that this is not an issue since Novell is no longer being used as of January 2000.

System User Access Controls

Organizations can reduce the risk of unauthorized changes or disclosures occurring by (1) granting employees authority to read or modify only those programs and data that are necessary to perform their duties, (2) periodically reviewing employees' authority and modifying it to reflect changes in job responsibilities, and (3) monitoring the use of the authority granted to ensure that it is being used only for the purposes authorized. Without effective access controls, the reliability of computer system data cannot be maintained, sensitive information data can be accessed and changed, and information can be inappropriately disclosed.

15. **Weakness:** NMVAHCS allowed 15 information resource management (IRM) staff to have special access privileges that allowed each of them to have access to the system account. With this system account, each of these users could obtain access to all financial and sensitive veteran information. While it is appropriate for selected computer staff to have broad access authority, we found that NMVAHCS did not have procedures to ensure that these IDs were adequately

controlled. Specifically, because NMVAHCS had not established appropriate control procedures, it did not:

- provide specific criteria for granting broad system access authority,
- require and maintain authorization documentation for all programmers as a permanent record of valid and approved access authority, including the purpose and time frames needed,
- periodically review each ID and recertify the continued need for this broad access, and
- routinely monitor user access activities to ensure that these powerful IDs were being used only for their intended purposes. (1999)

Recommendation: Establish and implement procedures to ensure that IDs with special access privileges are adequately controlled. Routinely monitor user access activities.

Management Response: In January 2000, NMVAHCS officials told us that they are planning to create and implement policies and procedures for system access that include criteria for granting broad access, maintaining authorization documentation, reviewing and recertifying authorization, and routinely monitoring user access activities. These actions will be completed by June 2000.

16. **Weakness:** A powerful user ID (postmaster) was shared by 15 staff, even though these staff members have individual accounts. This ID was being used to create new users, establish system options, and define security assignments. The use of shared IDs undermines the effectiveness of monitoring because individual accountability is lost. (1999)

Recommendation: Discontinue shared use of the powerful user ID.

Management Response: In January 2000, NMVAHCS officials told us that they have instructed staff to discontinue use of this powerful user ID and to use unique IDs when performing activities on the system. Existing policy will be updated in this regard by June 2000. Additionally, NMVAHCS told us that a software program had been developed to audit postmaster functions and is being run weekly.

17. **Weakness:** NMVAHCS did not adhere to formally documented procedures for granting access to NMVAHCS users. Specifically, NMVAHCS did not ensure that

- all signatures and approvals had been obtained prior to granting access to NMHCS systems,
- all access request forms included all information needed,
- request forms were maintained for all NMVAHCS users,
- user access was not granted based on phone requests, and
- periodic reviews or recertifications of user access were performed to ensure that individual business needs for system access continued to exist. (1999)

Recommendation: Establish a review process to ensure adherence to documented procedures for granting access.

Management Response: In January 2000, NMVAHCS officials told us that a review process will be established by June 2000 to ensure that procedures for granting access are followed.

Segregation of Duties

One fundamental technique for safeguarding programs and data is the appropriate segregation of duties and responsibilities of computer and financial personnel to reduce the risk that errors or fraud will go undetected. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed.

18. **Weakness:** Eleven staff involved with procurement had the ability to request, approve, and receive medical items without management approval. This violates the basic segregation of duties principle and VA policy. We found that from October 1998 through November 1999, 6 of the 11 staff requested, approved, and received 60 purchases totaling about \$300,000 in medical-related supplies. We found no evidence of NMVAHCS management approval of these purchases as prescribed by VA policy, nor did we find mitigating controls to alert management to purchases made in this manner. The continued practice of allowing fiscal agents to have total control of purchases increases the risk that inappropriate or fraudulent transactions could be processed, possibly without detection. Exacerbating the situation, 9 of the 11 staff also had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. (1999)

Recommendation: Establish a policy to (1) limit the ability of an individual to request, approve, and receive items and edit the vendor file and (2) develop a program for monitoring this activity.

Management Response: In January 2000, NMVAHCS officials told us that a medical center policy will be developed that regulates limitation of access, approval of access, and provides specifications for periodic review. This policy will be developed by June 2000. In addition, a local software program had been written to audit these activities. In February 2000, NMVAHCS told us that it had reviewed the 60 purchases and found no evidence of fraud or abuse. In addition, NMVAHCS officials stated that they had developed a software program for management purposes to audit and report on these types of purchase activities monthly.

Application Development and Change Control

Application development and change controls should be designed and implemented to prevent unauthorized programs or modifications to an existing program from being implemented. This is accomplished by instituting policies, procedures, techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

19. **Weakness:** There were no procedures for periodically reviewing Veterans Health Information Systems and Technology Architecture (VISTA) programs to ensure that only authorized program code was moved into production. Consequently, NMVAHCS increases its risk that unauthorized changes could be introduced into locally developed programs after they have been tested and approved but before the programs have been placed into production. NMVAHCS has access to a utility program that will allow it to identify unauthorized program changes that have been made to the VISTA production programs. (1999)

Recommendation: Establish procedures for periodically reviewing VISTA programs to ensure that only authorized program code is moved into production.

Management Response: In January 2000, NMVAHCS officials told us that they will establish and implement procedures for the periodic review of VISTA programs to ensure that only authorized program code is implemented. In February 2000, NMVAHCS told us that a local software program had been written to monitor computer application program changes and that this program was being run weekly.

Service Continuity

Service continuity controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. These controls include (1) procedures designed to protect information resources and minimize the risk of unplanned interruptions and (2) a well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

20. **Weakness:** Critical backup files for financial and sensitive veterans' medical programs, data, and software were not being stored off-site. In the event of a disaster to NMVAHCS's main computer facility, there are no assurances that all critical financial and sensitive medical systems can be fully restored. (1997)

Enclosure 1

Recommendation: Store critical backup files for financial and sensitive veterans' medical programs, data, and software off-site.

Management Response: In January 2000, NMVAHCS officials told us that they were reviewing alternatives for storing critical backup files off-site with VISN staff and plan to be in compliance with VISN specifications to be developed by April 2000.

21. **Weakness:** NMVAHCS was not performing periodic walk-throughs or unannounced tests of its disaster recovery plan. Conducting these types of tests provides a scenario more likely to be encountered in the event of an actual disaster. (1999)

Recommendation: Perform periodic walk-throughs or unannounced tests of the disaster recovery plan.

Management Response: In January 2000, NMVAHCS officials told us that walk-throughs of their disaster recover plan will occur quarterly beginning in February 2000.

Physical Security Access

Important information system controls for protecting access to data are the physical security control measures, such as locks, guards, and surveillance equipment, that an organization has in place. Such controls are critical to safeguarding critical financial and sensitive information and computer operations from internal and external threats. At NMVAHCS, we identified several areas where physical security could be improved.

22. **Weakness:** No formal procedures had been developed for granting access to the main computer room or for periodically reviewing user access. As a result, staff could be granted access or continue to have access to sensitive areas even though their job responsibilities might not warrant this access. (1999)

Recommendation: Develop and implement formal procedures for granting and periodically reviewing access to the main computer room.

Management Response: In January 2000, NMVAHCS officials told us that they will develop and implement policies and procedures for granting access to the computer room by May 2000.

23. **Weakness:** There were no procedures to periodically account for all keys to the computer room. We identified five keys to the information resource management area that were lost, including one for a door to the computer room that was not under camera surveillance. We also identified an additional computer room key assigned to an employee who no longer works at NMVAHCS. Until procedures

are developed to routinely account for all keys, NMVAHCS is at increased risk that physical security to the computer room will be compromised. (1999)

Recommendation: Establish and implement procedures to periodically account for computer room keys.

Management Response: In January 2000, NMVAHCS officials told us that the computer room will be rekeyed and policy will be developed and implemented to include procedures for periodically accounting for computer room keys. These actions will be completed by May 2000.

24. **Weakness:** Combustible materials were stored in the wiring closets. Storage of combustible materials in the wiring closets increases the risk that a fire could spread and cause injury to personnel and property damage. (1999)

Recommendation: Remove combustible materials from the wiring closets.

Management Response: In January 2000, NMVAHCS officials told us that all inappropriate material had been removed. Additionally, these areas will be regularly inspected beginning in March 2000.

Computer Security

Management

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

25. **Weakness:** NMVAHCS completed a risk assessment in November 1999 using a tool provided by VA's Medical Information Security Service. However, the tool was not designed to provide NMVAHCS with the information needed to establish controls to mitigate those risks identified with the highest vulnerabilities. We also plan to communicate this weakness to VA management.

In addition, NMVAHCS does not have a process, as required by VA policy, to assess risks when significant changes are made to its systems. For example, NMVAHCS has upgraded its computer hardware and added network capabilities since 1997. Each of these events should have warranted a separate risk assessment. (1997)

Recommendation: Establish a complete risk assessment framework that includes a process for assessing risk when significant system changes occur.

Management Response: In January 2000, NMVAHCS officials told us that procedures will be established by September 2000 for assessing risk when system changes occur, as required by VA policy.

26. **Weakness:** NMVAHCS had not developed a structured security training curriculum. The Computer Security Act of 1987 mandates that all federal employees who are involved with the management, use, or operation of federal computer systems be provided periodic training in computer security awareness and accepted computer security practices. Without a structured security training curriculum, NMVAHCS has no assurance that personnel involved in information system operations are adequately trained to identify threats and vulnerabilities and evaluate the adequacy of controls. (1999)

Recommendation: Develop a structured security training curriculum.

Management Response: In January 2000, NMVAHCS officials told us that they were in the process of developing and implementing a revised program for new employee orientation and mandatory security training by September 2000.

27. **Weakness:** The information security officer who performed security oversight for the Windows NT and VISTA systems as a collateral duty had not received security training in either of these systems. Without adequate training in these systems, the network security officer will be hampered in his or her efforts to provide adequate security oversight by his or her limited understanding of security controls designed for and configured in these systems. (1999)

Recommendation: Establish a technical security training program for the information security officer.

Management Response: In January 2000, NMVAHCS officials told us that they are establishing the information security officer as a full-time position. In conjunction with this position, they will establish a technical security training program by September 2000.

28. **Weakness:** NMVAHCS had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Our May 1998 study of security management best practices found that an effective control evaluation program includes processes for (1) monitoring compliance with established information system control policies and guidelines, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities.

As discussed in previous sections of this report, we found weaknesses that included inadequately limiting access to the network and not maintaining effective user IDs and passwords. These weaknesses could have been identified and corrected if NMVAHCS had been monitoring compliance with established

Enclosure 1

procedures. For example, periodically reviewing the network parameters for security vulnerabilities would have allowed NMVAHCS to discover and fix the type of network access control weaknesses we identified. Likewise, routinely reviewing passwords to monitor compliance with VA guidelines that prohibit the use of common words would mitigate some of the password security exposures we found. (1997)

Recommendation: Establish a program to routinely monitor and evaluate the effectiveness of the information system controls.

Management Response: In January 2000, NMVAHCS officials told us that they plan to establish a program to routinely monitor and evaluate the effectiveness of information system controls. Implementation of this program will be included in the duties and responsibilities of the information security officer's performance standards. They estimated that this issue would be resolved by September 2000.

**Computer Control Issues
That NMVAHCS Corrected**

The following table identifies the computer weaknesses we identified during our work at NMVAHCS during 1997. During our fieldwork, we determined that these weaknesses had been corrected by the center.

Corrected Weaknesses
Access controls-physical controls
1. Too many IRM staff had access to the computer room.
2. Criteria for gaining access to the computer room were not defined in NMVAHCS policy.
3. NMVAHCS did not have procedures for logging individuals who were escorted into the computer room.
Access controls-logical controls
4. The default Virtual Memory System (VMS) "field" account with privileges to all data and software used by the vendor was maintained in an active mode.
5. Two former IRM VMS users had system-level privileges.
6. The VMS "system" account with privileges to all data and software was shared with as many as 16 users.
7. Five VMS accounts, all with system-level privileges, did not have password expiration dates.
8. Veterans Health Information Systems and Technology Architecture (VISTA) accounts had a 10-second delay between password attempts.
Access controls-network controls
9. Fifteen accounts did not have passwords.
Segregation of duties controls
10. Nine current or former IRM users had unrestricted access to VISTA files and electronic signature keys.
Application change controls
11. NMVAHCS did not have formal procedures to review changes to core VISTA applications.
12. NMVAHCS did not have a policy for making local changes to VISTA applications.
Service continuity
13. NMVAHCS did not test the disaster recovery plan.
14. A copy of the disaster recovery plan was not maintained off site.
15. NMVAHCS did not have procedures to periodically review the disaster recovery plan.

Enclosure 3

GAO Contact and Staff Acknowledgments

GAO Contact

David W. Irvin, (214) 777-5716

Acknowledgments

In addition to the contact named above, Debra M. Conner, Denise Fitzpatrick, Jeffrey Knott, Norman Poage, Charles M. Vrabel, and Christopher J. Warweg made key contributions to this report.