GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284215

February 1, 2000

Mr. Alan G. Harper
Director, North Texas Health Care System
Department of Veterans Affairs
4500 South Lancaster Road
Dallas, Texas 75216

Subject: VA Systems Security: Information System Controls at the North Texas Health Care System

Dear Mr. Harper:

As part of our review of computer security at the Department of Veterans Affairs (VA), we assessed the effectiveness of information system general controls[1] at the North Texas Health Care System (NTHCS). 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 NTHCS 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 NTHCS 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 the 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 NTHCS's information system control policies and procedures. We also tested and observed the operation of information system controls over NTHCS's financial

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

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 NTHCS officials. Where those officials indicated that corrective actions had been taken, we observed and tested the controls placed into operation to assess their effectiveness.

NTHCS made progress in correcting specific computer security weaknesses that we identified in our previous evaluation of information system general controls. NTHCS had resolved 18 of our prior recommended actions, as well as three additional issues we identified during our most recent review. For example, NTHCS had reduced the number of users with certain powerful system privileges and limited access to the computer room to only those users who need it to carry out their assigned responsibilities. In addition, NTHCS established procedures to identify and delete unused or unneeded user identifications (ID) to its main computer system.

However, we identified continuing significant weaknesses that pose a risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and destruction of financial and sensitive veteran medical information. Specifically, we found that NTHCS had not established effective access controls over its network or adequately (1) managed network user IDs and passwords, (2) controlled remote access, or (3) monitored network system activity. In addition, NTHCS had not established procedures to control access by powerful user IDs to its main computer systems. Moreover, NTHCS had not adequately segregated security administration duties, provided for continued processing of its critical financial and sensitive medical systems in the event of service interruptions, or established comprehensive physical security controls. In all, our work identified 23 specific weaknesses, 20 of which remained open as of the end of our fieldwork.

NTHCS had established a foundation for implementing a computer security management program which included appointing a full-time security officer with specific roles and responsibilities, promoting security awareness, and developing a plan to review its security policies and procedures. However, NTHCS had not yet instituted a framework for continually assessing risks or routinely monitoring and evaluating the effectiveness of information system general controls. Our May 1998

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

study of security management best practices[4] found that both these missing elements are key ingredients in a comprehensive computer security management program which is essential to ensure that information system general controls work effectively on a continuing basis.

We are recommending actions to correct each of the remaining 20 individual weaknesses identified and described in more detail in enclosure I. Enclosure I describes the computer security weaknesses that remained open at the completion of our site visit and makes specific recommendations to resolve the weaknesses. Enclosure II summarizes the computer control weaknesses that NTHCS corrected.

NTHCS was responsive to addressing new security exposures identified during our recent review and corrected several weaknesses before our fieldwork was completed. In November 1999, NTHCS provided us with a corrective action plan to address the remaining weaknesses we identified. 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 these corrective actions but plan to do so as part of future reviews.

We performed our review at NTHCS, from October through December 1999, in accordance with generally accepted government auditing standards. On January 6, 2000, you and your executive office staff told us that you agreed with our findings. You stated that in many cases, NTHCS has subsequently corrected the reported computer security vulnerabilities and has a corrective action plan to resolve the remaining weaknesses by the end of the second quarter of fiscal year 2000.

We are sending a copy of this correspondence 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

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

any questions or wish to discuss this report, please contact me at (202) 512-3317. Key contributors to this report are listed in enclosure III.

Sincerely yours,

Robert F. Dacey

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

Enclosures

Computer Security Weaknesses at NTHCS That Remain Open

This enclosure summarizes the information system general control weaknesses we identified during our work at NTHCS 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 by types 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 networks. 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 though each NTHCS system may have its own level of security. As a result, financial information and sensitive veterans' medical information is at increased risk of unauthorized modification or disclosure occurring without detection.

Using network analysis software designed to detect network vulnerabilities, 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 which 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 November 1999, NTHCS told us it was working with the Hines Field Office (Office of the Chief Information Officer) to correct this problem by February 2000.

2. **Weakness:** A parameter that controls a system service was not configured to effectively prevent unauthorized access to a network system. As a result of this vulnerability, we were able to access sensitive files, including user and system information, without authentication. This would provide unauthorized users with information to gain access to the NTHCS network. (1999)

Recommendation: Configure system parameters to effectively prevent unauthorized access to the network system.

Management Response: In November 1999, NTHCS told us that it was working with the vendor to change the system settings and software by November 30, 1999.

3. **Weakness:** Certain network system software had not been updated to reflect the most recent vendor upgrades. This allowed us, as an unauthenticated user, to remotely gain high-level access, which would allow full control of the system and potential denial of service. (1999)

   Recommendation: Update system software to reflect the most recent vendor upgrades.

   Management Response: In November 1999, NTHCS told us that it was working with the vendor to change the system settings and software by November 30, 1999.

4. **Weakness:** On one network system, used to provide system access from remote locations, an optional system parameter had been enabled that allowed the system to automatically log on to an administrator account without user interaction. Because of ineffective system controls, we as an unauthenticated user were able to read the administrator ID and password. This weakness created a high-risk situation since administrator accounts typically have full control of the system. (1999)

   Recommendation: Disable system parameter that allows the system to automatically log on to an administrator account.

   Management Response: In November 1999, NTHCS told us that it was working with the vendor to change the system settings and software by November 30, 1999.

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

We found several examples where NTHCS was not adequately controlling IDs and passwords, including the following.

5. **Weakness:** Generic user IDs were being shared by an indeterminable number of users. NTHCS was not periodically reviewing user IDs to preclude the use of shared IDs. Use of these shared IDs undermines the effectiveness of monitoring because individual accountability is lost. (1999)

   Recommendation: Remove generic IDs from the system.

   Management Response: In November 1999, NTHCS told us that the generic IDs would be deleted by February 15, 2000.

6. **Weakness:** Approximately half of the network user IDs, including the network administrator user ID, were vulnerable to abuse because passwords were common words or characters that could be easily guessed or identified through commonly available hacker tools. NTHCS 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 November 1999, NTHCS told us that it had developed a security brochure to aid users in creating secure passwords and was adding this information to its New Employee Orientation program. In addition, a program to annually assess passwords would be established by the end of the second quarter of fiscal year 2000.

7. **Weakness:** At least 50 network users were using the default password or a slight variation. This increases the risk that a commonly known password could be used to obtain improper access to the NTHCS system. (1999)

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

   Management Response: In November 1999, NTHCS told us that it had developed a security brochure to aid users in creating secure passwords and was adding this information to its New Employee Orientation program. In addition, a program to annually assess passwords would be established by the end of the second quarter of fiscal year 2000.

8. **Weakness:** At least 23 network passwords 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 passwords. Consequently, there is greater risk of unauthorized use of passwords and user accounts to gain access to system resources. (1999)

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

Management Response: In November 1999, NTHCS told us that the expiration settings for these IDs had been changed to expire.

We also found that NTHCS was not promptly removing access authority for terminated or transferred employees, or deleting unused or unneeded IDS.

9. **Weakness:** We found that IDs belonging to terminated or transferred employees were not being disabled. We identified over 120 active IDs belonging to terminated or transferred employees. If user IDs are not promptly disabled when employees are terminated, former employees are allowed the opportunity to sabotage or otherwise impair NTHCS operations. (1999)

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

   Management Response: In November 1999, NTHCS told us that these IDs would be deactivated by February 15, 2000. In addition, NTHCS will periodically review IDs to identify terminated or transferred employees, and reemphasize policies and procedures for removal of IDs for terminated or transferred employees.

10. **Weakness:** We identified 69 IDs that had not been used for over 90 days. We also identified over 700 IDs that had never logged onto the network. Allowing this situation to persist poses unnecessary risk that unneeded IDs will be used to gain unauthorized access to NTHCS computer systems. (1999)

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

    Management Response: In November 1999, NTHCS told us that these IDs would be deactivated by February 15, 2000. In addition, NTHCS will periodically review user accounts and disable IDs that are unneeded.

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.

11. **Weakness:** NTHCS had not established remote access control policies or procedures to require that dial-in connections to internal systems and networks be authorized and to prohibit employees from connecting unauthorized modems to network workstations. NTHCS 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 November 1999, NTHCS told us that it would establish policy requirements for authorizing and reviewing dial-in connections from remote locations by November 30, 1999.

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 these controls, organizations have little assurance that unauthorized access to systems on its network would be detected in time to prevent or minimize damage.

12. **Weakness:** NTHCS did not have a proactive network-monitoring program to identify unusual or suspicious activities. Moreover, NTHCS did not have a policy that required procedures for event logging and maintaining audit trails of access activities that would warrant review. Although NTHCS was logging some of its network activities, key critical events were not being recorded. Also, these logs were not reviewed regularly and for those that had been reviewed, NTHCS 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. In addition, although VA has procedures for reporting computer security incidents, these procedures will not be effective until NTHCS establishes a mechanism for identifying computer security incidents, which can only be accomplished through a network-monitoring program. At the end of our fieldwork, NTHCS had begun using a network audit tool to review its system and security logs. (1997)

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

Management Response: In November 1999, NTHCS told us that it would establish a monitoring program to review access for unusual or suspicious activities by the second quarter of fiscal year 2000.

User Access Controls

Organizations can reduce the risk that unauthorized changes or disclosure occur by (1) granting employees authority to read or modify only those programs and data that are necessary to perform their duties, (2) periodically reviewing this 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 a computer system's data cannot be maintained, sensitive information data can be accessed and changed, and information can be inappropriately disclosed.

13. **Weakness:** NTHCS allowed 12 programmers to have powerful IDs, which allowed them to access all financial and sensitive veteran information maintained on NTHCS's main computer systems. While it is appropriate for selected computer staff to have broad access authority, we found that NTHCS did not have procedures to ensure that these IDs were adequately controlled. Specifically, NTHCS did not perform the following control procedures.

    - 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.

    - Routinely monitor user access activities to ensure that these powerful IDs are being used only for their intended purpose. (1999)

    Recommendation: Establish and implement procedures to ensure that access authorization documents are maintained and periodically recertified. Routinely monitor user access activities.

    Management Response: In November 1999, NTHCS told us that it will obtain signed access authorization documents for all programmers by December 30, 1999, and will begin annual reviews of programmer access. In addition, it plans to perform random audits on programmer activities to include integrity checks on critical routines. The first audit is planned for January 2000.

Segregation of Duties

One fundamental technique for safeguarding programs and data is the appropriate segregation of duties and responsibilities of computer and security personnel to reduce the risks that errors or fraud will go undetected.

14. **Weakness:** At NTHCS, the security officer reports to the director of Information Resource Management (IRM). As a consequence, the security officer may not have full independence when assessing security within the IRM function. The computer security function could be improved either through organizational change or by establishing procedures to ensure that the security officer can perform his duties independently and through management oversight of this function. (1999)

    Recommendation: Take appropriate steps to ensure independence of the security officer.

    Management Response: In November 1999, NTHCS told us that it would establish procedures to ensure that the security officer had the system access needed to perform independent security reviews. In addition, NTHCS management said it would perform routine management oversight to ensure the independence of the security function.

<u>Service Continuity</u>

An organization must ensure that it is adequately prepared to cope with a loss of operational capabilities due to tornadoes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for catastrophes is a current, complete, and fully tested service continuity plan for information resource services. Such a plan is critical for ensuring that information systems can promptly restore operations and data in the event of disaster.

In reviewing service continuity at NTHCS, we found several areas where improvements were needed, including the following.

15. **Weakness:** The service continuity plan was not complete. It did not include provisions for recovery of all mission critical systems, including the network and NT systems. Until a service continuity plan is completed, the facility may not be able to recover critical operations in the event of a disaster. (1999)

    Recommendation: Complete the service continuity plan to include provisions for recovery of all mission critical systems, including network and NT systems.

    Management Response: In November 1999, NTHCS told us that complete service continuity plans to include all its network systems would be developed by the end of the second quarter of fiscal year 2000.

16. **Weakness:** Annual testing of the service continuity plan had not been performed as required by VA and VHA policy. Testing the service continuity plan is essential to ensure that all procedures required for restoring data processing capabilities and mission-critical applications have been included in the plan. Until it tests the service continuity plan, NTHCS has no assurance that, in the event of a disaster, it will be able to fully restore all critical financial and sensitive medical systems. (1997)

Recommendation: Annually test the service continuity plan.

Management Response: In November 1999, NTHCS told us that a program to annually test its service continuity plan would be established by the end of the second quarter of fiscal year 2000.

Physical Security Controls

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 NTHCS, we identified several areas where physical security could be improved.

17. **Weakness:** Sensitive cables and wiring panels in the NT room were not adequately protected to prevent disruptions to computer operations. The cables and wiring panels were exposed to daily walk-through traffic, increasing the risk that either could be damaged and thus result in possibly severe and lengthy disruptions and loss of data. (1997)

    Recommendation: Protect sensitive cables and wiring panels in the NT room.

    Management Response: In November 1999, NTHCS told us that it would reposition cables on the floor and, where practical, utilize cable ties to better protect exposed cables by November 30, 1999.

18. **Weakness:** No formal procedures had been developed for granting 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. (1997)

    Recommendation: Implement formal procedures for granting access to the main computer room.

    Management Response: In November 1999, NTHCS told us that procedures for granting computer room access would be implemented by November 30, 1999.

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 planning and management program, staff (1) periodically assess risks, (2) implement comprehensive policies and procedures, (3) promote security awareness, (4) monitor and evaluate the effectiveness of the computer security environment, and (5) maintain a central security function to provide computer security guidance and oversight.

As we recommended in our fiscal year 1997 review, NTHCS established a foundation for its computer security planning and management program by appointing a full-time security officer with specific roles and responsibilities, promoting security awareness, and developing a plan to review its security policies and procedures. However, NTHCS had not yet implemented all key elements of a comprehensive security planning and management program including the following areas.

19. **Weakness:** NTHCS completed a risk assessment in September 1999 using a tool provided by the VA's Medical Information Security Service. However, the tool was not designed to provide NTHCS 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, NTHCS had no process to assess risk when significant changes are made to its systems as required by VA policy. For example, NTHCS had upgraded its computer hardware and added network capabilities since 1994. Each of these events would have warranted a separate risk assessment. (1999)

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

    Management Response: In November 1999, NTHCS told us it would update its security plan to include a complete risk assessment framework by the end of the second quarter of fiscal year 2000.

20. **Weakness:** NTHCS had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Our May 1998 study of best practices in the area of security management 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 (1) inadequately limiting access to the network and (2) maintaining effective user IDs and passwords. These weaknesses could have been identified and corrected if NTHCS had been monitoring compliance with established procedures. For example, periodically reviewing the network parameters for security vulnerabilities would have allowed NTHCS 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 English words would mitigate some of the password security exposures we found. (1999)

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

Management Response: In November 1999, NTHCS told us that a program to routinely monitor and evaluate the effectiveness of information system controls would be established by the end of the second quarter of fiscal year 2000.

Computer Control Weaknesses That NTHCS Corrected

The following table shows the computer control weaknesses we identified during our work at NTHCS during 1997 and 1999 that had been corrected by the center before we completed our fieldwork in 1999.

Corrected Weakness	Year Identified
Access controls – physical controls	
1. All NTHCS Information Resource Management (IRM) staff had access to the computer room.	1997
2. NTHCS did not have procedures for periodically reviewing access to the computer room.	1997
3. Windows in the NTHCS computer room were not alarmed.	1997
4. Surveillance camera was not positioned correctly to provide a clear visual image of individuals entering the computer room.	1999
Access controls – logical controls	
4. One vendor Virtual Memory System (VMS) system account with privileges to all data and software was not deactivated when not needed and had only a five-position password.	1997
5. Seven IRM staff had access to all Veterans Health Information Systems and Technology Architecture (VISTA) resources and VMS system-level privileges (three staff had not used VMS in over a year).	1997
6. Over 160 staff with VMS access had no documentation to support privileges granted.	1997
7. The VMS system account with privileges to all data and software was shared with an undetermined number of users. This did not provide for individual accountability for system actions.	1997
8. Twelve VMS accounts with system level privileges had no identifiable owners.	1997
9. One hundred twenty-four VMS accounts, including 9 with system level privileges, did not have password expiration dates.	1997
10. Nineteen VMS accounts had password expiration dates of over 90 days.	1997
11. Seven Integrated Data Communication Utility (IDCU) accounts for terminated employees were still active.	1999
12. Eight hundred and fifteen VISTA accounts (access codes) and 44 VMS accounts had not been used in 90 days.	1997
13. Over 90 VISTA accounts and 6 Austin Automation accounts for terminated or transferred employees were still active.	1997
Access controls – network controls	
14. User passwords were not required to be periodically changed.	1997
15. User passwords were not required to have expiration dates.	1997
16. Warning banners for network access did not include all information required to inform users of the legal consequences of unauthorized use of network resources.	1997

Corrected Weakness	Year Identified
Application change controls	
17. NTHCS did not have formal procedures to comprehensively review changes to core VISTA applications.	1997
Service continuity	
18. A copy of the disaster recovery plan was not maintained off-site.	1997
19. NTHCS did not maintain backup files off-site.	1999
20. NTHCS did not have procedures to periodically review the disaster recovery plan.	1997
Computer Security Management	
21. NTHCS did not have a full-time information security officer.	1997

GAO Contact and Staff Acknowledgements

GAO Contact

David W. Irvin, (214) 777-5716

Acknowledgements

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

(919454)