United States General Accounting Office

GAO

Report to the Secretary of the Interior

July 2001

INFORMATION SECURITY

Weak Controls Place Interior's Financial and Other Data at Risk

GAO-01-615

GAO
Accountability * Integrity * Reliability

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

July 3, 2001

The Honorable Gale A. Norton
The Secretary of the Interior

Dear Madam Secretary:

We reviewed information system general controls[1] over the financial systems maintained by the Department of the Interior at its National Business Center (NBC) in Denver, CO. Effective information system general controls are critical to NBC-Denver's ability to safeguard assets and ensure the confidentiality and reliability of financial management information. Such controls also affect the security and reliability of nonfinancial information, such as personnel information maintained by NBC-Denver. Additionally, NBC-Denver uses its information systems to provide computer processing services to other federal agencies.

Our review of Interior's information system general controls was performed in connection with the department's financial audit conducted under the Chief Financial Officers Act of 1990, as expanded by the Government Management Reform Act of 1994. Our evaluation included follow-up on the computer security weaknesses previously identified by Interior's Office of Inspector General (OIG). The results of our evaluation of information system general controls were shared with Interior's OIG for its use in auditing Interior's consolidated financial statements for fiscal year 2000.

This report provides a general summary of the weaknesses we identified and our resulting conclusions and recommendations. We are also issuing today a report designated for "Limited Official Use," which describes in more detail the computer security weaknesses identified and offers specific recommendations for correcting each. After we completed our

[1]Information system 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 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.

fieldwork and orally informed the acting assistant director of NBC-Denver of the identified weaknesses, he provided us with information regarding corrective actions taken or planned. Although these actions are noted in this report, we have not yet evaluated their effectiveness.

Results in Brief

Although NBC-Denver has made progress in correcting the computer security weaknesses previously identified by the OIG and has taken other steps to improve security, we identified additional weaknesses in NBC-Denver's information system control environment. These weaknesses affected the center's ability to (1) prevent and detect unauthorized changes to financial information, including payroll and other payment data, (2) control electronic access to sensitive personnel information, and (3) restrict physical access to sensitive computing areas. The effect of these weaknesses is to place sensitive NBC-Denver financial and personnel information at risk of unauthorized disclosure, critical financial operations at risk of disruption, and assets at risk of loss. These weaknesses and risks also affect other agencies that use computer processing services at NBC-Denver.

NBC-Denver did not adequately limit access granted to authorized users, control all aspects of the system software controls, or secure access to its network. Also, NBC-Denver had not fully established a comprehensive program to routinely monitor access to its computer facilities and data and to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. Further, NBC-Denver was not providing adequate physical security for its computer facility, appropriately segregating computer functions, effectively controlling changes to application programs, or fully ensuring that all aspects of its service continuity needs were addressed.

A primary reason for NBC-Denver's information system general control weaknesses was that it had not yet fully developed and implemented a comprehensive entitywide program to manage computer security. An effective program would include issuing guidance and procedures for assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and evaluating the effectiveness of established controls. While NBC-Denver has implemented a security awareness program and taken other actions to improve security management, it still needs to take additional steps to address the other key elements of a computer security management program. Such a program, if fully and effectively implemented, would

provide NBC-Denver with a solid foundation for resolving existing computer security problems and continuously managing information security risks.

To improve information system general controls over NBC-Denver financial operations, we are recommending that NBC-Denver correct the computer security weaknesses identified and implement an effective entitywide computer security management program. The acting assistant director of NBC-Denver stated that he has agreed to correct the weaknesses that we identified, and at the completion of our fieldwork, he provided us with a comprehensive corrective action plan to address each of them.

In commenting on a draft of this report, the Acting Assistant Secretary for Policy, Management, and Budget agreed with our recommendations. He noted that approximately 50 percent of the recommendations had already been implemented and that all of them would be implemented by December 31, 2001.

Background

NBC-Denver is a service center operated by the Department of the Interior. NBC-Denver develops and operates administrative and financial systems (including payroll/personnel, administrative payments, accounts receivable, property management, and accounting) for the Department of the Interior as well as more than 30 other federal organizations, under cross-servicing agreements. During fiscal year 2000, NBC-Denver reported processing more than $9 billion in payroll payments for more than 200,000 employees from federal organizations, including the Department of Education, Social Security Administration, and Pension Benefit Guaranty Corporation. The center also provided accounting and financial reporting services to the department and other federal agencies. For fiscal year 2000, NBC-Denver reported processing more than 3 million nonpayroll financial transactions totaling more than $3 billion.

At the time of our review, NBC was migrating several systems from its Reston, VA, service center to its Denver facility. NBC-Reston was responsible for operating the department's standardized accounting system, which supports six Interior bureaus, seven other federal activities, and the department's procurement system. As a result of this migration, completed in January 2001, NBC-Denver will be responsible for providing all centralized administrative and financial processing to department

bureaus and offices. NBC-Reston will continue to be responsible for providing functional support for the department's systems.

NBC-Denver is operated by the Office of the Secretary. The center relies on a nationwide telecommunications network that links computer hardware at remote locations serving the Department of the Interior's 14 bureaus and offices to the NBC-Denver mainframe computers. In addition, many of the other federal organizations that NBC-Denver supports have direct communications to link them with the center's computers. At the time of our review, there were about 37,000 users with access to NBC-Denver systems.

Objective, Scope, and Methodology

Our objective was to evaluate the design and test the effectiveness of information system general controls over the financial systems maintained and operated by the Department of Interior at its NBC-Denver data center. These information system general controls also affect the security and reliability of other sensitive data, including personnel information maintained on the same computer system as the department's financial information.

Specifically, we evaluated information system general controls intended to

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

To evaluate these controls, we identified and reviewed NBC-Denver policies and procedures, conducted tests and observations of controls in operation, and held discussions with NBC-Denver staff to determine whether information system general controls were in place, adequately designed, and operating effectively. In addition, we reviewed the Department of the Interior's OIG reports on information system general controls performed in connection with the department's annual financial statement audits for fiscal years 1996 through 1999. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*

(FISCAM),[2] which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data, and (2) our May 1998 report on security management best practices at leading organizations,[3] which identifies key elements of an effective information security program.

We did not perform a review of information system general controls at NBC-Reston because at the time of our review, the key systems maintained at this center were in the process of being migrated to NBC-Denver.

We performed our work at NBC-Denver from October 2000 through February 2001. Our work was performed in accordance with generally accepted government auditing standards.

We requested comments on a draft of this report from the Department of the Interior. The department provided us with written comments, which are discussed in the "Agency Comments" section and reprinted in appendix I.

Improvements Made in Security, but Systems Remain Vulnerable

In 1997 and again in 1998, Interior's OIG, in connection with the department's required annual financial statement audit, reported on computer security weaknesses at NBC-Denver. Among the specific weaknesses reported were those related to limiting access granted to authorized users, properly managing user IDs and passwords, adequately controlling changes to system and application software, and completely developing its business recovery plan. These weaknesses placed critical department operations, such as financial management, personnel, and other operations, at greater risk of misuse and disruption. NBC-Denver has made progress in correcting the weaknesses identified by the OIG and has taken other steps to improve security.

Although NBC-Denver had addressed weaknesses found by the OIG, we identified additional control weaknesses in NBC's information systems. Specifically, NBC-Denver had not adequately limited the access granted to

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

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

all authorized users, controlled all aspects of the system software environment, or completely secured access to its network. The risks created by these access control weaknesses were heightened because the center had not established a comprehensive program for routinely monitoring access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. Consequently, financial, payroll, and personnel programs and data maintained at NBC-Denver are at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction, which may occur without detection.

NBC-Denver Had Acted to Improve Security

NBC-Denver had made progress in addressing computer security issues previously identified and reported on by Interior's OIG in connection with the department's 1997 and 1998 annual financial statement audits. For example, the center had

- limited access to certain sensitive access privileges to critical programs, software, and data;
- improved user ID and password management controls on its mainframe computer;
- updated its service continuity plan and developed a business recovery plan;
- performed a risk assessment of its major applications;
- established a computer security awareness program for its employees; and
- developed and performed comprehensive tests of its computer security disaster recovery plans.

In addition, during the past 3 years, NBC-Denver initiated other steps to improve computer security. These efforts included (1) review of system software; (2) improvements in physical security, including the addition of a guard service, installation of camera surveillance, and use of electronic access cards; (3) review of system user access; and (4) installation of intrusion detection software to monitor network access.

Access Authority Was Not Appropriately Limited for All Users

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modifications, disclosure, or deletion. Organizations can protect this critical information by granting employees authority to read or modify only those programs and data that they need to

perform their duties and by periodically reviewing access granted to ensure that it is appropriate.

A key weakness in NBC-Denver's controls was that the center had not sufficiently restricted user access. While NBC-Denver had restricted access to many users who previously had broad access to critical programs, software, and data, we found instances where the center had not sufficiently restricted access to only legitimate users, including those described below.

- About 400 users had access privileges to four sensitive system software libraries that are allowed to perform sensitive system functions that can be used to circumvent all security controls. Such access increased the risk that users could bypass security controls to alter or delete any computer data or programs on the system and should only be granted to system programmers. This risk was further heightened because the center had not established mitigating controls ,such as monitoring user access to these sensitive libraries. The acting assistant director of NBC-Denver acknowledged that many of these users did not require access.
- About 1,000 users were given broad access privileges to a system software resource that allows users to create and modify programs and read and copy any data set to which such users have been granted read access. Such access is generally used for program development and testing. About 500 of the users were using this resource to run a set of standard programs, a task that does not require this level of access. With broad access privileges, users with knowledge of the security system could create and modify computer programs and read and copy sensitive data.
- Seventeen system maintenance staff had access that allowed them to alter or update system software resources used to control the storage of system and data files. This control function is an automated process that does not require users to have this type of access. With this access, users could move sensitive files to unprotected areas and modify or delete financial or sensitive data or disrupt computer operations.
- About 80 application developers, both programmers and functional specialists, had update access to payroll and personnel data. An essential control for ensuring the integrity of a computer application is to prevent software developers from having access to application programs and data in the production environment. Developers with detailed knowledge of the system's processing functions could improperly add, alter, or delete payroll and personnel data and programs without leaving evidence that the system had been compromised.

One reason for NBC-Denver's user access vulnerabilities was that access authority was not being reviewed on a periodic basis. Such reviews would have allowed the center to identify and correct inappropriate access.

In February 2001, the acting assistant director of NBC-Denver told us that the center was reviewing staff access and would limit staff access to the level required to carry out job responsibilities. Further, he said that the center would develop and implement procedures by October 2001 to periodically review access lists to ensure that access remains appropriate.

All System Software Controls Were Not Adequate

To protect the overall integrity and reliability of information systems, it is essential to control access to and modifications of system software. System software controls, which limit and monitor access to the powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. To protect system software, a standard computer control practice is to (1) configure system software to protect against security vulnerabilities, (2) periodically review programs in sensitive software libraries to identify potential security weaknesses, and (3) ensure that only authorized and fully tested system software is placed in operation.

While NBC-Denver had performed reviews of its system software environment and corrected those security weaknesses identified, we identified other areas where the center was not adequately controlling system software. These system software control weaknesses could diminish the reliability of financial and other sensitive information maintained on this computer system. We found the following weaknesses:

- A weakness in the system software configuration could allow knowledgeable users with access privileges that permit them to execute programs to bypass access controls and gain unauthorized access to sensitive financial and personnel information. In this case, the operating system was set up so that programs in any of 34 libraries included in the normal search sequence[4] could perform sensitive system functions and operate outside security software controls. This increases the risk that if unauthorized programs are introduced users could bypass other access

[4]The search sequence is used by the operating system to find and execute programs.

controls and improperly access or modify financial, audit trail, or other sensitive information maintained on the computer system.

- About 8,200 programs in sensitive software libraries, which have the authority to perform sensitive functions that can circumvent security controls, did not have unique program names. While multiple versions of the same software are maintained by NBC-Denver to satisfy customer requirements, an undetermined number of programs do not have unique program names. Allowing more than one program in these libraries to have the same name could lead to inadvertent or deliberate execution of an unauthorized program that could compromise security controls. NBC-Denver had not established a process to periodically review programs in sensitive libraries for security weaknesses, such as programs with duplicate names. Until NBC-Denver begins to actively review programs in sensitive libraries, it will not have adequate assurance that other security controls cannot be bypassed.
- Although NBC-Denver had a process for making changes to system software, it had not established written procedures or guidance for system software changes and had not developed guidance for testing changes or documenting test results. An essential control in the system software change process is that written procedures are established that set forth requirements for requesting, authorizing, and approving these changes. These procedures should include requirements for testing, performing a technical review, and obtaining approval for each system software change before implementation. During fiscal year 2000, NBC-Denver made more than 200 system software changes. Our review of a random sample of 20 changes for this period found that changes did not include documentation for (1) tests on 13 changes, (2) technical reviews of 16 changes, or (3) supervisory approvals on 16 software changes. Consequently, NBC-Denver faces increased risks of unintended operational problems caused by programming errors or the deliberate execution of unauthorized programs.

In February 2001, the acting assistant director of NBC-Denver told us that the center would implement additional policies and procedures, by October 2001, to (1) review system configuration settings periodically for security vulnerabilities, (2) evaluate programs in sensitive system libraries to identify and correct security exposures, and (3) document that system software changes are tested, technically reviewed, and approved before implementation.

Network Security Was Not Sufficient

Network security controls are key to ensuring that only authorized individuals can gain access to sensitive and critical agency data. These controls include a variety of tools, such as user IDs and passwords, which are intended to authenticate authorized users who access the network from local and remote agency locations and through dial-in facilities. In addition, network controls provide for safeguards to ensure that the system software is adequately configured to prevent users from bypassing network access controls or causing network failures.

The risks introduced by the weaknesses that we identified in access and system software controls were compounded by network security weaknesses: NBC-Denver was not adequately protecting access to its network or restricting access to the system that processes financial and other sensitive information. Specifically, the center had not adequately managed user IDs and passwords, controlled dial-in access, or adequately configured all its network servers. Thus, sensitive financial information processed on the network is at increased risk that unauthorized modification or disclosure could occur without detection. Because of NBC's interconnected environment, these network control weaknesses also increase the risk of unauthorized access to financial and other sensitive information (such as payroll, personnel, and financial management information) maintained on the NBC-Denver mainframe computer. For example,

- The network had user ID and password management weaknesses that an intruder could exploit to gain unauthorized access to the NBC-Denver network. For example, on one network server, we identified easily guessed passwords and passwords that had not been used since 1998. On another network, network commands available to all users allowed access to a listing that included password information.
- An ID and password used for dial-in access to the centralized modem pool was easily guessed. We were able to guess a user ID and password that provided an access path into the network. With this access we were able to browse the internal network and collect information about the network, which could be used to identify and exploit network vulnerabilities. The lack of adequate dial-in access controls increases the risk that a hacker could obtain access to the network, from which an attack could be launched on the mainframe to gain access to critical financial and sensitive department information. NBC-Denver staff corrected this network vulnerability before we completed our fieldwork.

- The network had system software configuration weaknesses that could allow users to bypass access controls and gain unauthorized access to NBC-Denver networks or cause network system failures. For instance, certain network systems configuration settings allowed unauthorized users to connect to the network without entering a valid user ID and password combination. This could allow unauthorized individuals to obtain access to system information describing the network environment, including user IDs and password information.

These network security weaknesses increased the risk that someone could gain unauthorized access to information on the network and that intruders or authorized users with malicious intent could exploit the network weaknesses to misuse, improperly disclose, or destroy financial and other sensitive information.

In February 2001, the acting assistant director of NBC-Denver told us that all accounts that had not been used within the prior 90 days had been deleted. Also, the acting assistant director told us that all test accounts and other easily guessed passwords had been removed. In addition, he stated that network system software configurations were reviewed and changes made to limit security vulnerabilities. Further, he informed us that policies and procedures had been developed and implemented to periodically review network password settings, accounts, and network system software configurations.

Program to Monitor Access Activities Was Not Complete

The risks created by the access control problems described above were heightened because NBC-Denver had not yet established a comprehensive program to monitor user access. Such a program would include routinely reviewing user access activity to identify and investigate failed attempts to access sensitive data and resources, as well as unusual and suspicious patterns of successful access to sensitive data and resources. Such a program is critical to ensuring that improper access to sensitive information is detected.

The most effective monitoring efforts are those that selectively target unauthorized, unusual, and suspicious patterns of access to sensitive data and resources, such as security software, system software, application programs, and production data. While the center had begun to review failed attempts to access sensitive system resources (e.g., security software and sensitive system software), it had not established a program to monitor successful access to production resources, including application programs

and data. Thus, there is an increased risk that application developers with access to production programs and data could add, alter, or delete payroll and personnel information (for example) without being detected, since these types of user activities were not being monitored. In addition, although NBC-Denver was reviewing access to certain system software, its process did not include logging all critical activities, such as access violations to or modifications made to all sensitive system libraries.

While NBC-Denver had installed an intrusion detection system to monitor access to its network, it had not established procedures for managing this system. For example, it had not established procedures for (1) determining where on its network it will monitor access, (2) protecting intrusion data from tampering, and (3) classifying, storing, analyzing, and using intrusion data to identify agency network vulnerability patterns. Further, it had not established procedures for following up and reporting on system anomalies or computer misuse after initial alarms are triggered. Without procedures for addressing these types of activities, NBC-Denver reduces its ability to establish and maintain an effective intrusion detection program, which reduces the risk of unauthorized access of computer resources.

In February 2001, the acting assistant director of NBC-Denver told us that by January 2002, the center would expand its user access monitoring program to include all sensitive system libraries and critical application production programs and data. Further, he stated that the center planned to develop and implement procedures for managing its intrusion detection program and reporting the results of unusual or suspicious access activities.

Other Information System Controls Were Not Sufficient

In addition to the information system access controls discussed above, other important controls should be in place to ensure the integrity and reliability of an organization's data. These information system controls include policies, procedures, and control techniques to physically protect computer resources and restrict access to sensitive information, provide appropriate segregation of duties of computer personnel, prevent unauthorized changes to application programs, and ensure the continuation of computer processing operations. We found weaknesses in each of these areas.

Physical Security Controls Were Not Adequate

Physical security controls are 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 they are housed and periodically reviewing access granted to ensure that it continues to be appropriate. At NBC-Denver, physical access control measures (such as locks, guards, badges, and alarms, used alone or in combination) are vital to safeguarding critical financial and sensitive personnel information and computer operations from internal and external threats.

Although NBC-Denver policy requires a photo access card to gain access, via electronically controlled doors, to the building that contains the computer center, we observed on different occasions that several people entered the building by merely following one person with an authorized access card. While guards were posted at the entrance to the building, we observed that they were not checking each person entering the building for an appropriate NBC-Denver photo access card. Thus, individuals who did not have NBC-Denver photo access cards could pass unchallenged through the main entry doors and gain unauthorized access to the facility, increasing the risk that intruders with malicious intent might obtain access to sensitive computer resources or disrupt operations.

Further, we identified 40 employees and contractors, including mail room, facility support, computer support, tape librarian, local-area network (LAN) support, and personnel/payroll staff, who had access to the electrical room. This room contains fiber optic boxes that could be used by a knowledgeable person to establish an unauthorized internal connection to the center's computer system. While it is appropriate for facility and computer support staff to have access to the electrical room, care should be taken to limit access to only those staff who need access to perform their job responsibilities. NBC-Denver had not established policies and procedures for granting access to the electrical room.

We also determined that the center had not restricted physical access to a console in the tape library with master console authority, which could be used to issue sensitive operator commands. Although at the time of our review this console had only recently been moved to its temporary location, the area was unprotected and provided an opportunity for unauthorized individuals entering the building to use the console to issue commands that could disable security access checking or cause the system to fail. Allowing unrestricted access to this console increased the risk of unauthorized access to NBC-Denver systems and disruption of services.

In February 2001, the acting assistant director of NBC-Denver told us that a policy would be developed and implemented to ensure that photo identification access cards would be checked on all individuals entering the facility that houses the main computer. In addition, the acting assistant director told us that a policy for granting and periodically reviewing access to the electrical room would be developed. Further, the acting assistant director told us that the master console command capabilities were removed from the operator console in the tape library in December 2000.

Computer Duties Were Not Always Properly Segregated

Another fundamental technique for safeguarding programs and data is to segregate the duties and responsibilities of computer personnel so as to reduce the risk that errors or fraud will occur and go undetected. Incompatible duties that should be separated include application and system programming, production control, database administration, computer operations, and data security. Once policies and job descriptions supporting the principles of segregation of duties have been developed, it is important to ensure that adequate supervision is provided and adequate access controls are in place to ensure that employees perform only compatible functions.

Although computer duties were generally properly segregated at NBC-Denver, we identified instances where controls did not enforce segregation of duties principles. For example, two application support staff had access privileges that allowed them to modify financial production programs and data as well as security-related information. These staff were assigned responsibility for performing certain functions related to security administration and production program maintenance. Under normal circumstances, staff with security responsibilities should report to the security administrator and have no programming duties. However, because these individuals had both program and security administration access privileges, they had the ability to change programs and data and eliminate any evidence of their activity in the system. Compounding this risk, NBC-Denver was not monitoring the system activities of these individuals. Allowing staff the capability to modify financial programs and security information without compensating controls increases the risk of unauthorized modification of critical financial data.

In addition, NBC-Denver did not provide supervisory oversight to its computer operators on selected weekend shifts, nor was it routinely reviewing the console activity logs for these shifts to ensure that only authorized operational activities were being conducted. Controls over

personnel activities require active supervision and review of these activities. To aid in this oversight, all computer operator activities on the computer system should be recorded on an automated history log; this log should be reviewed routinely by supervisory staff and any abnormalities investigated. Because these controls were not implemented, NBC-Denver increased its risk that unauthorized activities could occur on these shifts without detection.

In February 2001, the acting assistant director of NBC-Denver told us that the two application staff would be given access to a second user ID so that they could perform certain needed operational functions on an ad hoc basis. This ID will be tightly controlled, requiring management approval for its use and audit recording and review of all access activities. Further, the acting assistant director told us that lead operators were being added to those shifts where only one operator was assigned. The lead operator would also be responsible for reviewing all changes made at the system console.

Changes to Application Programs Were Not Adequately Controlled

It is important to ensure that only authorized and fully tested application programs are placed in operation. To ensure that changes to application programs are needed, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, as part of the application change control process, library management software should be used to control program versions, and test procedures should be established to ensure that only authorized changes are made to program code.

Changes to application programs at NBC-Denver were not adequately documented or controlled. Described below are several examples of application change control weaknesses.

- Although a change control board at NBC-Denver was responsible for authorizing all application changes, the authorizations for these changes were not formally documented. For example, in a random sample of 20 application changes made during fiscal year 2000, none of the changes had formal documentation to show that the software modifications had been authorized by the change control board.
- Documentation was not always maintained to provide evidence of the specific program modifications made or their approval. Specifically, the change control documentation for 13 of the 20 changes that we

reviewed did not include a description of the specific modifications made to the program code or evidence of supervisory approval.
- NBC-Denver did not use automated library management software to ensure that program versions were not accidentally misidentified and to avoid simultaneous changes to the same program.
- Procedures were not in place to periodically test program code to ensure that only authorized changes had been made.

Without a clearly defined and implemented application change control process, changes may be implemented that are not authorized, tested, documented, or approved. Further, NBC-Denver is at greater risk that software supporting its operations will not produce reliable data or effectively meet operational needs.

In February 2001, the acting assistant director of NBC-Denver told us that a form would be developed and attached to each modification request to (1) document authorization for program changes, (2) record a description of the change made, (3) identify program modules modified, and (4) provide for the signature of the reviewing official. Also, he stated that NBC-Denver would perform program code reviews to ensure that only authorized program changes are made.

Service Continuity Planning Was Not Complete

An organization must take steps to ensure that it is 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 disaster recovery plan that covers all key computer operations and includes plans for business recovery. Such a plan is critical for helping to ensure that information system operations and data, such as financial processing and related records, can be promptly restored in the event of a disaster. To ensure that it is complete and fully understood by all key staff, the disaster recovery plan should be tested annually and the test plans and results documented to provide a basis for improvement. In addition, critical computer data and programs should be stored off site and periodically inventoried.

While NBC-Denver had conducted comprehensive tests of its computer center disaster recovery plan, improvements are still needed in some areas of its overall plan, including the business recovery plan. Described below are examples of service continuity weaknesses identified at NBC-Denver.

- NBC-Denver had not conducted unannounced tests or walk-throughs of its disaster recovery plan. Instead, all tests had been planned with participants fully aware of the disaster recovery test scenario. In an actual disaster, there is usually little or no warning.
- Critical backup files for financial and sensitive agency personnel programs, data, and software stored off site were not inventoried. As a result, if a disaster befell the center's main computer facility, there are no assurances that all critical and sensitive system resources would be available to fully restore all key systems.
- NBC-Denver had not tested its business recovery plan annually as required by the center's plan. The plan has not been tested since October 1999. Conducting tests of the plan serves to reinforce staff roles and responsibilities in a disaster and in the process provides greater assurance that business operations will be restored if a disaster occurs.

In February 2001, the acting assistant director of NBC-Denver told us that the center will begin performing periodic walk-throughs of its various disaster recovery plans by October 1, 2001. Also, policy and procedures will be developed that will require a semiannual inventory of programs, data, and software files stored off site. Further, he stated that center staff will ensure that the NBC-Denver business recovery plan is tested at least annually, as required by the existing NBC-Denver procedures.

Computer Security Management Program Is Essential

A key reason for NBC-Denver's weaknesses in information system controls was that it had not yet fully developed and implemented a comprehensive entitywide security management program to ensure that effective controls were established and maintained and that computer security received adequate attention. 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.[5] An effective computer security management program would include

- establishing a central security management staff that provides guidance and oversight for the computer security management program,
- performing periodic risk assessments,
- establishing appropriate policies and procedures,
- raising security awareness, and

[5]GAO/AIMD 98-68.

- evaluating the effectiveness of established controls.

NBC-Denver had taken action related to each of the key elements described above, including the implementation of a comprehensive security awareness program both for employees and contractors. However, aside from security awareness, the steps taken to address the other key elements of a comprehensive security management program were not sufficient to ensure the continuing success of the program.

The first key element of effective computer security management is the establishment of a central security group. This function serves to provide overall security policy and guidance for the organization. In addition, it provides the oversight to ensure compliance with established policies and procedures and reviews the effectiveness of the security environment.

NBC-Denver had not established a central computer security management staff. Instead, NBC-Denver relied on the IT security manager and certain staff assigned to the network, facilities, and application functions to perform security tasks. Although these staff had general department guidance on information security, NBC-Denver had not developed specific policies and procedures that clearly defined the security roles and responsibilities of these staff and the reporting lines between the security functions. In addition, there were no specific procedures requiring these staff to coordinate on security-related issues, such as policy development and implementation, risk assessment, monitoring compliance with established policies and procedures, and reviewing the effectiveness of controls.

A second key aspect of computer security management is periodically assessing risk. Regular risk assessments assist management in making decisions on necessary controls by helping to ensure that security resources are effectively distributed to minimize potential loss. Also, by increasing the awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure that the policies and controls operate as intended.

Although Department of the Interior policy requires that risk assessments be performed whenever significant changes are made to a facility or its computer systems, but at least every 5 years, NBC-Denver had not developed a framework for assessing and managing risk when significant changes occurred. During the past year, the center upgraded its mainframe operating system and added servers to its network. Each of these events

was a significant change that warranted a separate risk assessment. However, while NBC-Denver had performed risk assessments for part of the key applications, it had not performed a risk assessment when these significant changes occurred.

A third key element of effective security management is having established policies and procedures governing a complete computer security program. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local area network, wide area network, and mainframe security. The integration of network and mainframe security is particularly important as computer systems become more and more interconnected.

NBC-Denver had not yet established comprehensive policies and procedures to govern a complete computer security program. While the center had made progress in developing policies and procedures for specific security areas, including remote dial-in access, the network firewall, incident response capability, and user ID and password management, it had not developed an overall policy on computer security. This policy would address security requirements for physical and logical access control, segregation of duties, application change control, service continuity, and security management covering both network and mainframe environments. In addition, NBC-Denver had not developed technical standards for implementing security software and maintaining operating system integrity on either its mainframe or network systems. Such standards would not only help ensure that appropriate computer controls are established consistently, but would also facilitate periodic reviews of these controls.

A fourth key area of security program management is promoting security awareness. Computer attacks and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer systems in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality and integrity. In accepting responsibility for security, employees should, for example, devise effective passwords, change them frequently, and protect them from disclosure. In addition, employees should help maintain physical security over their assigned areas.

NBC-Denver had established a security awareness program for all its employees and contractors. Specifically, NBC-Denver developed a computer-based security awareness program that all of its employees and contractor staff are required to complete annually. Further, NBC-Denver had established procedures to monitor compliance with this requirement.

A final key area of an overall computer security management program is an ongoing security oversight program. Such a program includes processes for (1) monitoring compliance with established information system control policies and procedures, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities.

NBC-Denver had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Such a program would allow NBC-Denver to ensure that policies remain appropriate and that controls accomplish their intended purpose.

Weaknesses discussed in this report could have been identified and corrected if the center had been monitoring compliance with established procedures. For example, if NBC-Denver had periodically reviewed user access authority to ensure that it was limited to the minimum required access level based on job requirements, the center would have been able to discover and limit the access of application development staff to sensitive system resources. Likewise, routinely evaluating the technical implementation of its system software would have permitted the center to eliminate or mitigate the additional system software exposures discussed in this report.

A program to regularly test information system controls would also have allowed NBC-Denver to detect additional network security weaknesses. For example, using network analysis software designed to detect network vulnerabilities, we identified user accounts and services that could provide hackers with information to exploit the network and launch an attack on NBC-Denver systems. Although NBC-Denver fixed this problem before our fieldwork was completed, center staff could have identified and corrected this exposure using similar network analysis software available to them.

In February 2001, the acting assistant director of NBC-Denver told us that a security oversight team would be established to coordinate overall security at the center. In conjunction with this effort, he said that policies and procedures would be developed and implemented that define the roles and

responsibilities of all NBC-Denver functions involved in security management. These policies and procedures will include requirements for coordinating security activities among the designated security functions. He added that NBC-Denver will develop a framework for risk assessments, including a policy and procedures for performing risk assessments for the physical facility, application, and computer center environments. In addition, the acting assistant director told us that his staff was currently developing a comprehensive site security policy that will include technical standards for each operating computer platform. He also said that the center will develop a security oversight program to monitor compliance with established information system control policies and procedures, test the effectiveness of information system controls, and improve information system controls based on the results of these activities. These computer security management elements are to be implemented no later than October 2001, according to the acting assistant director.

Conclusions

Information system general controls are critical to NBC-Denver's ability to ensure the reliability of Interior's financial management information and maintain the confidentiality of sensitive personnel and other department information. While NBC-Denver has made progress in correcting the computer security weaknesses that Interior's OIG identified and has taken other steps to improve security, additional weaknesses were identified in NBC-Denver's information system control environment. Specifically, NBC-Denver had not adequately limited users access, controlled system software, secured network access, or established a program to comprehensively monitor access. Also, NBC-Denver was not providing adequate physical security, segregating computer functions, controlling changes to application programs, or ensuring that all aspects of its service continuity needs were addressed. These weaknesses placed sensitive NBC-Denver financial and personnel information at risk of disclosure, critical financial operations at risk of disruption, and assets at risk of loss. These weaknesses could also affect other agencies that depend on NBC-Denver's computer processing services.

A primary reason for NBC-Denver's information system control weaknesses was that it had not yet fully developed and implemented a comprehensive computer security planning and management program. A comprehensive program for computer security management is essential for achieving an effective information system general control environment. Effective implementation of such a program provides for periodically assessing risks, implementing effective controls for restricting access

based on job requirements and actively reviewing access activities, communicating the established policies and controls to those who are responsible for their implementation, and perhaps most important, evaluating the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose.

The acting assistant director of NBC-Denver stated that he has recognized the seriousness of the weaknesses we identified and at the completion of our fieldwork provided us with a comprehensive corrective action plan to address each of them.

Recommendations for Executive Action

To establish an effective information system general control environment, we recommend that you instruct the Director of the National Business Center and the acting assistant director of NBC-Denver, in coordination with the Interior Chief Information Officer (CIO), to ensure that the following actions are completed.

- NBC-Denver corrects the information system control weaknesses related to access authority, system software, network security, access monitoring, physical access, segregation of duties, program changes, and service continuity. These specific weaknesses are described in a separate report designated for "Limited Official Use," also issued today.
- NBC-Denver develops and implements an effective computer security management program. Such a program would include (1) establishing a central security group to manage a cycle of security management activities, (2) assessing risk to determine computer security needs, (3) developing and implementing policies and controls that meet these needs, and (4) instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

In addition, we recommend that you instruct the Interior CIO, as the department's key official responsible for computer security, to report periodically to you, or your designee, on progress in implementing Interior's corrective action plans.

Agency Comments

In commenting on a draft of this report, the Acting Assistant Secretary for Policy, Management, and Budget agreed with our recommendations. He reported that to date, approximately 50 percent of the recommendations

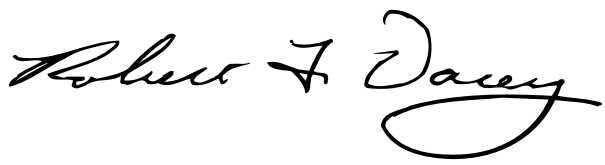
made had been implemented, and that action on all of them would be completed by December 31, 2001.

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 to the Senate Committee on Governmental Affairs and the House Committee on Government Reform not later than 60 days after the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with 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 Conrad Burns, Senator Robert C. Byrd, Senator Joseph Lieberman, Senator Ted Stevens, Senator Fred Thompson, Representative Dan Burton, Representative Norman Dicks, Representative Joe Skeen, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of the Senate and House Committees. We will also send copies to Mitchell E. Daniels, Jr., Director, Office of Management and Budget; Robert J. Lamb, Acting Assistant Secretary for Policy, Management and Budget, Department of the Interior; Daryl W. White, Chief Information Officer, Department of the Interior; Timothy G. Vigotsky, Director of the National Business Center; and Earl E. Devaney, Inspector General of the Department of the Interior. Copies will also be made available to others upon request and will be available on our home page at http://www.gao.gov.

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. We can also be reached at daceyr@gao.gov and irvind@gao.gov. Key contributors to this report are listed in appendix II.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

Comments From the Department of the Interior

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

JUN 14 2001

Mr. Joel Willemssem
Managing Director, Information Technology
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Willemssem,

Thank you for the opportunity to respond to the draft report entitled, "Information Security Weak Controls Place Interior's Financial and Other Data at Risk". We concur with the recommendations contained in the report, including correction of the weaknesses identified. As your report indicates, we have developed a comprehensive plan to address correction of those weaknesses.

We also want to express our appreciation for the professionalism and the thoroughness that GAO has displayed in the conduct and reporting of this audit. The GAO staff, through its technical competency and spirit of cooperativeness, have identified several areas where NBC-Denver can improve its general controls. Your recommendations will further our efforts to ensure that our customers' financial, payroll/personnel, and other sensitive data are adequately protected from fraudulent or unauthorized use.

In the thirteen years that the NBC Denver Center has been in operation, we have continuously strived to create controls that provide a secure environment for customer data. While audits do identify opportunities for improvement, the impetus for security controls has always been internally driven. We take information system controls very seriously. As your staff identified weaknesses, we took immediate action to mitigate our more sensitive exposures. We are aggressively moving to correct all of the weaknesses identified in the draft report. To date, approximately 50% of the recommendations made by GAO have been implemented; approximately 65 % will have been completed by July 1; approximately 80% of the recommendations will have been implemented by October 1; and we will have completed all of the recommendations identified in the report by

December 31, 2001. It includes the recommended improvements to our comprehensive program for computer security management. In addition, all but one of the weaknesses identified in the 1997 and 1998 Department OIG audits referenced in your report were corrected prior to this audit. The remaining weakness was corrected in April, 2001.

As the report indicated, NBC-Denver has initiated a number of information system controls in the areas of computer and network security. To protect our sensitive and financial data, we have instituted a multi-layered security environment composed of network security controls, system security controls, and application security controls. This redundancy is to assure that a breach in one of the security layers (e.g., network security) does not easily lead to unauthorized access to data unless all three layers are circumvented (e.g., system and application security). We are continuously seeking ways to improve security controls in all three areas; network, system, and application security.

As part of its overall security management program, NBC-Denver has recognized the importance of periodically performing risk assessments. NBC-Denver has been performing risk assessments of its data center since 1990 and its major applications since 1992. These assessments have been performed in accordance with OMB Circular A-130, National Institute of Standards and Technology (NIST), and Department of the Interior requirements. Based on the results of these assessments, existing information system controls are modified to protect the integrity, confidentiality, and accessibility of the computerized data. We recognize the need to continuously perform risk assessments as changes occur to the information systems and physical environment.

NBC-Denver has pro-actively taken measures to assure a successful recovery of operations should a disaster occur. We have developed and performed walkthroughs of our Business Recovery Plan. We have extensively tested our ability to recover computer operations at our computer hot site. NBC-Denver performs full image backups (i.e. all programs and data) on a weekly basis and sends these backups to an off-site storage facility. We receive a report of the number of tape storage containers that the off-site facility receives upon the vendor's receipt of the containers. The tape storage containers are kept locked from the time that we put the tapes in the containers until the time that the tapes are returned to NBC-Denver. The possibility of a tape being lost is virtually non-existent. Additionally, we inventory the tapes during disaster recovery testing (twice each year).

While this audit, as well as previous audits, have identified areas where NBC-Denver can improve its management controls, none of these audits has ever shown that the integrity of the financial data has ever been compromised. Our on-going operations have provided our customers accurate financial information and timely delivery of services.

We appreciate the constructive input by your staff and the opportunity to provide comments on the audit recommendations. If you have questions or concerns, please contact Rick Koebert, Acting Assistant Director, Products and Services, NBC at (303) 969-7210.

Sincerely,

Robert Lamb

Robert Lamb
Acting Assistant Secretary
Policy, Management and Budget

GAO Contact and Staff Acknowledgements

GAO Contact

Dave Irvin, (214) 777-5716

Acknowledgements

In addition to the person named above, Edward Alexander, Lon Chin, Debra Conner, Denise Fitzpatrick, Edward Glagola, David Hayes, Sharon Kittrell, Jeffrey Knott, West Coile, Harold Lewis, Suzanne Lightman, Duc Ngo, Tracy Pierson, Norman Poage, and Charles Vrabel 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)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00