United States General Accounting Office

GAO

Report to the Secretary of Agriculture

July 1999

USDA INFORMATION SECURITY

Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure

GAO/AIMD-99-227

GAO
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-283156

July 30, 1999

The Honorable Dan Glickman
The Secretary of Agriculture

Dear Mr. Secretary:

We reviewed information system access controls[1] over the financial information systems maintained by the Department of Agriculture (USDA) at its National Finance Center (NFC), which is located in New Orleans, Louisiana. Our work was done in cooperation with the USDA Office of Inspector General's internal control audit of NFC, which was part of its audit of USDA's fiscal year 1998 consolidated financial statements.

NFC develops and operates administrative and financial systems for USDA and other federal organizations under cross-servicing or franchising agreements. Access controls are critical to NFC's ability to safeguard assets and ensure the confidentiality and reliability of financial management information. Such controls, however, also affect the security and reliability of nonfinancial information, such as personnel information, maintained by NFC.

Today, we are also issuing a report designated for "Limited Official Use," which details weaknesses in access controls over NFC computer systems. This version of the report, which was excerpted for public release, provides a general summary of the weaknesses we identified and the recommendations we made. After we completed our fieldwork, the director of NFC provided us with updated information regarding corrective actions. However, these reported actions, which are noted in this report, will need to be verified to ensure that they are operating effectively.

[1]Access controls are a component of information security designed to protect computer resources from unauthorized modification, loss, or disclosure. They include logical, system software, and physical controls. Logical controls prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems. Physical controls limit access to computer facilities and associated resources.

Results in Brief

Serious access control weaknesses affected NFC's ability to prevent and/or detect unauthorized changes to payroll and other payment data or computer software, control electronic access to Thrift Savings Program account information, and restrict physical access to sensitive computing areas. These weaknesses increased the risk that users could cause improper payments. In addition, sensitive information contained in NFC systems, including financial transaction data and personnel information, was vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. Furthermore, NFC payroll processing and other financial management operations were vulnerable to disruption due to these weaknesses.

We found significant problems related to the center's control and oversight of access to its systems and the data maintained on these systems. NFC was not adequately limiting the access of authorized users or controlling its operating system software to prevent access controls from being circumvented. For several years, the Office of Inspector General has reported that access control procedures were weak. The access control weaknesses we identified were further compounded because NFC was not sufficiently protecting or overseeing access to its network. In addition, the center was not providing adequate physical security for its computer resources.

The access control weaknesses we found indicate that NFC's computer security planning and management program had not adequately ensured that information system controls continued to work effectively. An effective program would include guidance and procedures for assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls.

Importantly, NFC management has recognized the seriousness of the weaknesses we identified and expressed its commitment to improving information system controls. In commenting on this report, the director of NFC agreed with our findings and recommendations. The director also stated that NFC had corrected most of the information security weaknesses we identified and planned actions to address remaining weaknesses. In addition, NFC stated that it intends to strengthen its computer security planning and management program to encompass the best practices described in our May 1998 report. Addressing these issues

will help ensure that an effective computer security environment is achieved and maintained.

Background

The National Finance Center develops and operates administrative and financial systems, including payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems for both USDA and more than 60 other federal organizations, including GAO, under cross-servicing or franchising agreements. During fiscal year 1998, NFC processed more than $19 billion in payroll payments for more than 450,000 employees from federal organizations including the Secret Service, Internal Revenue Service, and Drug Enforcement Administration. The center also serviced more than $1 billion in accounts receivable and processed more than 450 million accounting transactions in fiscal year 1998.

NFC is also responsible for maintaining records for the world's largest 401(k)-type program, the federal Thrift Savings Program. This program, which is growing at about $1 billion per month, covers about 2.3 million employees and totaled more than $60 billion as of September 30, 1998.

NFC is operated by USDA's Office of the Chief Financial Officer (OCFO) in New Orleans, Louisiana. The center relies on a nationwide telecommunications network that links computer hardware at remote locations to the NFC mainframe computers. Certain financial applications, such as the Purchase Card Management System that manages around $34 million in payments, are also processed on the network.

Objective, Scope, and Methodology

Our objective was to evaluate the design and test the operational effectiveness of access controls over the financial systems maintained and operated by USDA at NFC. We evaluated controls intended to protect data and application programs from unauthorized access. Specifically, we reviewed

- the technical implementation of NFC's security software and other system software,
- network access controls, and
- physical access controls.

We restricted our evaluation at NFC to these controls because USDA's Office of Inspector General planned to review the other information system general controls[2] as part of the fiscal year 1998 internal control audit of NFC.

To evaluate access controls, we identified and reviewed NFC policies and procedures related to access control, conducted tests and observations of controls in operation, and held discussions with NFC staff to determine whether access controls were in place, adequately designed, and operating effectively. Our evaluation was based on the guidance provided in our Federal Information System Controls Audit Manual (FISCAM)[3] and the results of our May 1998 study of security management best practices at leading organizations.[4] We performed our work from July 1998 through February 1999 in accordance with generally accepted government auditing standards.

After we completed our fieldwork, the director of NFC provided us with updated information regarding corrective actions. However, these reported corrective actions will need to be verified to ensure that they are operating effectively.

USDA provided us with written comments on a draft of this report, which are discussed in the "Agency Comments" section and reprinted in appendix I.

[2]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.

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

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

Information in NFC Systems Was Vulnerable to Unauthorized Access

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. Our review of NFC's access controls found that the center was not adequately protecting financial and sensitive personnel information. Specifically, NFC had not appropriately limited access granted to authorized users, effectively controlled its operating system software, sufficiently secured access to its network, or adequately restricted physical access to its computer resources. As a result, NFC's computer systems, programs, and data are at risk of inadvertent or deliberate misuse, fraudulent use, unauthorized alteration, or destruction possibly occurring without detection.

NFC management has recognized the weaknesses we identified and has expressed its commitment to improving information system controls. We have noted those instances where management has implemented corrective actions or indicated that corrective actions are planned. A summary of the weaknesses follows.

Access Authority Was Not Appropriately Limited for Authorized Users

A key weakness in NFC's access controls was that the center had not sufficiently restricted the access for authorized users. Organizations can protect information from unauthorized changes or disclosures by granting employees authority to read or modify only those programs and data that are necessary to perform their duties and periodically reviewing access granted to ensure that it is appropriate. NFC, however, had not adequately limited access to financial and sensitive personal information maintained on its systems. We found several examples, detailed below, where NFC had not sufficiently restricted access authority for legitimate users.

- Eighty-six user IDs had an access privilege that allows users to read and alter any data stored on tape regardless of other security software controls. These users included staff from the Accounting Systems Branch, the Foundation Financial Information System Development team, and the Financial Reporting team. As a result, these users have access to all NFC tape files, including payroll files. Although this privilege is generally required to process tapes received from external organizations**,** it should be limited to one group, such as the tape library group, that copies external tapes to the format required by NFC for processing. In April 1999, the director of NFC told us that actions had been taken to limit this access privilege to 20 technical employees, with only 1 having the ability to update all tapes.

- More than 60 mainframe user IDs enabled users to update a sensitive system file that controlled certain access privileges and files containing audit trail information. Allowing such broad access to these files increases the risk that users could circumvent the security software and alter or delete audit trail information. In April 1999, the director of NFC told us that this access had been removed from all individuals.
- Sensitive system files on a network system were not adequately protected from unauthorized users. These files could be exploited using readily available "hacker" tools to gain access to this system, which could lead to improper payments related to the Purchase Card Management System.

System Software Controls Were Not Effective

In addition to restricting user access authority, controls over access to and modification of system software are also essential to protect the overall integrity and reliability of information systems. System software controls limit and monitor access to the powerful programs and sensitive files associated with computer system operation. Generally, one set of system software is used to support and control all of the applications that run on the system. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

System software controls are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. If controls in this area are not adequate, system software might be used to bypass security controls or gain unauthorized privileges to perform unauthorized actions or circumvent edits and other controls built into application programs. We found that NFC was not properly controlling system software to prevent access controls from being circumvented. Such weaknesses diminish the reliability of information produced by all applications supported by the computer system and increase the risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and disruption.

We identified the following system software configuration weaknesses that could allow users to bypass access controls and gain unauthorized access

to financial and other sensitive information maintained at NFC or cause system failures.

- A system software component that could be used to bypass security access controls and alter data, programs, and audit trail information was available to all users who could submit a program for batch processing.[5] As a result, all information, including payroll, personnel, and investment data, was at risk of unauthorized modification and deletion occurring without detection. NFC staff subsequently modified this component to prevent security controls from being circumvented.
- The system software that controls batch processing allowed any user with the ability to execute a batch program to also use any operator command without intervention. Allowing such broad access to operator commands that can turn off other components of the system software, such as the security software, or cause the system to stop increases the risk that operations could be severely disrupted. NFC staff restricted the ability to execute operator commands through batch programs within 2 hours of our telling them about this problem.
- Versions of at least seven network system software programs with known vulnerabilities that could be exploited to gain unlimited access to the network had not been updated or disabled to prevent unauthorized access. These exposures could allow unauthorized users to obtain access privileges that would allow them to bypass security controls. In April 1999, the director of NFC told us that his staff had begun correcting these vulnerabilities and planned to complete this process by the end of July 1999.

In addition, NFC had not instituted a process to periodically review programs in certain system software libraries, which are allowed to perform sensitive functions that can be used to circumvent all security controls and to identify and correct weaknesses. Until NFC begins actively managing programs in sensitive system libraries, the center will not have adequate assurance that mainframe security controls cannot be bypassed. In April 1999, the director of NFC told us that the center had established a process to monitor programs in sensitive system software libraries.

[5]Batch processing is a mode of computer operation in which transactions are accumulated over a period of time and then processed at one time. Users do not interact with the system while their programs are processing in batch mode.

Network Security Was Not Sufficient

The risks created by these access control problems were heightened because NFC was not sufficiently protecting access to its network. Specifically, NFC had not adequately managed user identifications (ID) and passwords, controlled access to its systems from remote locations, or monitored system activity. Thus, sensitive financial information processed on the network, including the Purchase Card Management System payments, is at increased risk of unauthorized modification or disclosure occurring without detection. Because of NFC'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 investment data, maintained on the NFC mainframe computer.

Network Password Management Controls Were Not Effective

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

We found several weaknesses relating to network password management.

- Seventy-six network IDs did not require passwords, which makes them more susceptible to misuse because user authentication is not required. More than 50 of these IDs were especially vulnerable because the account identifiers were common words, software product names, or derivations of words or products that could be easily guessed. In April 1999, the director of NFC told us that a password is now required for all user IDs.
- Seventy-seven network IDs were allowed to reuse the same password, which enables these IDs to circumvent password change requirements. This increases the risk that a password could be discovered and used to obtain improper access to the NFC system. In April 1999, the director of

NFC told us that all user IDs are now required to have a unique password.

- Sixteen network IDs were not disabled after a specified number of invalid password attempts. Allowing unlimited attempts to guess passwords increases the risk of unauthorized access to the NFC network and the financial information processed on the network. In April 1999, the director of NFC told us that these accounts are now disabled after five unsuccessful attempts are made to access them using invalid passwords.

Remote Access Was Not Adequately Controlled

Organizations must also control access to computer resources from remote locations to protect sensitive information from improper modification, disclosure, or destruction by outside 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[6] and telephone lines centrally, establish controls to verify that dial-in connections are authorized, and test for unauthorized modems. We found that NFC could not ensure that dial-in access was adequately secured. These weaknesses, along with the user ID and password problems described above, significantly increase the risk that unauthorized users could gain access to the NFC network.

NFC had drafted a network and personal computer security policy that acknowledged that dial-in access to a network or personal computer could subject critical applications and mainframe systems to unauthorized modification, deletion, and disclosure, and required dial-in access to be secured through passwords or dial-back[7] features. However, the security group was not involved in approving modem usage at NFC. In addition, although NFC planned to centralize control of dial-in access to minimize individual modems, only 16 of the 230 modems were controlled through a central system where user authentication was assured. NFC did not have procedures in place to ensure that dial-in access was adequately protected for the remaining 214 modems. Furthermore, NFC did not have a process in

[6]A modem is a device that allows digital signals to be transmitted and received over analog telephone lines.

[7]A dial-back system requires a user initiating a call to a network or workstation to provide a confidential code. The system then terminates the call and dials back to a previously specified location to complete the dial-in connection.

place to periodically reassess dial-in access to ensure that it was still required.

In April 1999, the director of NFC told us that his staff would remove all individual modems and provide dial-in access through a secured modem pool. The director also stated that formal guidance on modem usage would be included in the NFC network security policy, which is scheduled to be issued later in 1999.

Network Security Monitoring Program Was Not Effective

The risks created by these network access control problems were exacerbated because NFC did not have a proactive network monitoring program. Such a program would require NFC to promptly identify and investigate unusual or suspicious network activity indicative of malicious, unauthorized, or improper activity, such as repeated failed attempts to log on to the network, attempts to identify systems and services on the network, connections to the network from unauthorized locations, and efforts to overload the network to disrupt operations. Network monitoring programs should also include provisions for logging and regularly reviewing network access activities. Without these controls, NFC has little assurance that unauthorized access to systems on its network would be detected in time to prevent or minimize damage.

Although NFC had begun planning for a network monitoring program, it had not implemented a network intrusion detection system capable of detecting attacks on a real-time basis. Such a system would require NFC to identify suspicious access patterns and set up the intrusion detection system to automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

Also, NFC could not ensure that network attacks would be detected because the center was not monitoring network access activity. Although the draft local area network and personal computer security policy described procedures for event logging and audit trails, this policy did not include requirements for logging access to sensitive data and resources or reviewing access to these resources for unusual or suspicious activity. Furthermore, despite the requirements in the draft policy, NFC was not logging security events on its main operational network even though this is the primary means of identifying unauthorized users or unauthorized usage of the system by authorized users.

In April 1999, the director of NFC told us that his staff plan to implement a comprehensive network intrusion detection program by the end of July

1999. The director also stated that security logging and monitoring policies and practices would be established in the network security policy, which is scheduled for issue later in 1999.

Physical Security Controls Were Not Adequate

Physical controls are also important for protecting access to computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms where these resources are stored. At NFC, physical access control measures, such as locks, guards, badges, and alarms, (used alone or in combination), are critical to safeguarding critical financial and sensitive personnel information and computer operations from internal and external threats. However, NFC had not adequately controlled access to computer resources.

We found that more than 120 people, including maintenance and nontechnical support staff, had access to the computer room and tape library. At NFC, this unnecessary access not only increased the risk of inadvertent or deliberate damage to computer resources, but also heightened the risk of unauthorized changes to data stored on tape. In April 1999, NFC management told us that the center had eliminated unrestricted access to the computer room and tape library for maintenance and nontechnical support staff, who are now admitted by authorized staff members when access is required.

We also determined that physical access to a console, which could be used to issue sensitive operator commands, had not been restricted. Consequently, anyone could use this console to issue commands that would disable security access checking or cause the system to fail. Allowing unrestricted access to this console increases the risk of unauthorized access to NFC systems and disruptions in service. In April 1999, the director of NFC told us that constructing a separate room for this console is cost prohibitive; therefore, his staff plans to replace the terminal that provides these functions with a personal computer that will be password protected.

Computer Security Planning and Management Program Was Not Adequate

Our May 1998 study of security management best practices pointed out that a comprehensive computer security planning and management program is essential to ensure that information system controls continue to work effectively. However, the access control weaknesses we identified indicate that NFC's computer security planning and management program had not ensured that effective controls were established and maintained. The USDA Office of Inspector General has also reported since 1996 that access controls to prevent unauthorized access to or modification of sensitive data at NFC were weak. In addition, USDA began reporting inadequate computer security and application controls at NFC as a material weakness in its Federal Managers' Financial Integrity Act[8] report in 1998.

We found weaknesses in the design of NFC's computer security planning and management program. Under an effective computer security planning and management program, staff (1) periodically assess risks, (2) implement comprehensive policies and procedures, (3) promote awareness of prevailing risks and mitigating controls, and (4) monitor and evaluate the effectiveness of established controls. In addition, a central security staff is important for providing guidance and oversight for the computer security planning and management program to ensure an effective information system control environment. We found that NFC had not instituted a sufficient framework for managing information system controls or monitoring their effectiveness on an ongoing basis.

One key aspect of effective security planning and management is establishing appropriate 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 network and mainframe security. The integration of network and mainframe security is particularly important as computer systems become more and more interconnected. However, we found that NFC had not finalized its network security policy, which was drafted in 1996 and did not include provisions for an intrusion detection system. Furthermore, the USDA Office of Inspector General reported in March 1998 that NFC policies and procedures relating to physical security were not sufficient. In April 1999, the director of NFC told us that his staff was updating its draft Network and Personal Computer Security Policy to address the current

[8]The Federal Managers' Financial Integrity Act of 1982 requires agencies to establish controls that reasonably ensure that assets are safeguarded against waste, loss, or unauthorized use.

network architecture and environment and plan to issue the updated policy later in 1999.

In addition, NFC had not established a comprehensive program to evaluate the effectiveness of controls and compliance with established security policies and procedures. For example, we found that NFC did not have a network self-assessment program in place even though the network security environment is a dynamic one. Although NFC had performed some self-assessments in the beginning of 1998 to identify network security vulnerabilities, the program had not been formalized to ensure periodic self-assessments. Consequently, these self-assessments ceased when the staff member who had been performing them left NFC. We also found that certain policies and procedures were not being followed. For example, we found that certain NFC systems did not present an adequate warning to discourage unauthorized use on the initial screen because the warning required by NFC Directive 70 was not used on all systems.

In July 1999, NFC management told us that the center had installed software and implemented a network self-assessment program. The director also told us, in April 1999, that the Network and Personal Computer Security Policy, which is scheduled for release later in 1999, would define an adequate and consistent warning banner to be used on initial screens.

Conclusions

Access controls are critical to NFC's ability to ensure the reliability of financial management information and maintain confidentiality of sensitive information. However, NFC's access control problems placed sensitive personnel information at risk of disclosure, critical financial operations at risk of disruption, and assets at risk of loss. The access control weaknesses we identified could have also adversely affected other agencies that depend on NFC for computer processing support.

Implementing more effective and lasting controls that protect payments and sensitive personnel information and maintain an effective general computer control environment requires that NFC establish a comprehensive computer security planning and management program. This program should provide for periodically assessing risks, implementing effective controls for restricting access based on job requirements and proactively reviewing access activities, communicating the established policies and controls to those who are responsible for their implementation, and, perhaps most important, monitoring and evaluating

the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose.

NFC management has recognized the weaknesses we identified and has expressed its commitment to improving information system controls.

Recommendations

We recommend that the Secretary of Agriculture direct the Chief Financial Officer to take the following actions.

- Correct the specific access control weaknesses we identified and communicated to NFC management during our testing. These weaknesses are summarized in this report and detailed in a separate report, which is designated for "Limited Official Use," also issued today.
- Ensure that an effective entitywide security planning and management program, as described in our May 1998 study of security management best practices, is in place at NFC. Such a program would include
  - assessing risks periodically to determine needs and select cost-effective policies and related controls,
  - implementing policies and controls that are based on risk,
  - communicating the policies and controls, as well as the risks that prompted their adoption, to those responsible for complying with them,
  - evaluating the effectiveness of policies and related controls, and
  - establishing a central security management focal point to ensure that major elements of the security planning and management program are carried out and provide a communications link among organizational units.

Agency Comments

In commenting on a draft of this report, NFC agreed with our findings and recommendations. NFC stated that it had corrected most of the information security weaknesses we identified and planned actions to address remaining weaknesses. In addition, NFC stated that it intends to strengthen its computer security planning and management program to encompass the best practices described in our May 1998 report.

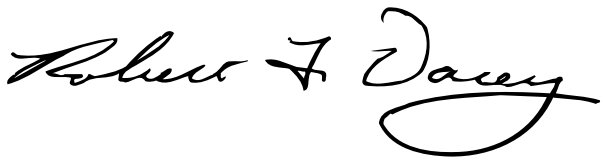
This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental

Affairs and the House Committee on Government Reform and Oversight 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 the agency's first request for appropriations made more than 60 days after the date of this report.

We are sending copies of this report to Senator Fred Thompson, Senator Joseph Lieberman, Representative Dan Burton, Representative Larry Combest, Representative John R. Kasich, Representative John M. Spratt, Jr., Representative Charles W. Stenholm, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of Senate and House Committees and the Honorable Jacob J. Lew, Director of the Office of Management and Budget. Copies will also be made available to others upon request.

Please contact me at (202) 512-3317 if you or your staff have any questions concerning this report. Key contributors to this report are listed in appendix II.

Sincerely yours,



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

Comments From the Department of Agriculture

USDA

United States Department of Agriculture

Office of the Chief Financial Officer

National Finance Center

P.O. Box 60000
New Orleans
Louisiana 70160

JUN 2 9 1999

Jeffrey C. Steinhoff
Acting Assistant Comptroller General
Management Division
U.S. General Accounting Office
441 G Street, NW, Room 5061
Washington, D.C. 20548

Dear Mr. Steinhoff:

We appreciate the opportunity to comment on the General Accounting Office's (GAO) draft report on information system controls at the National Finance Center (NFC). Your report cites several specific access control weaknesses which the NFC takes very seriously. We agree with the issues GAO identified and the recommendations contained in the report. The NFC immediately began to address these deficiencies as soon as they were communicated to us. We have already completed corrective actions on most of the items and have planned appropriate corrective actions on the rest.

As Director of the NFC, I recognize the importance of adequate security controls to protect the data assets of the customers we serve. In this rapidly changing technical environment, we can only achieve the level of safeguard required through a carefully managed process that is monitored for effectiveness. We appreciate the role that GAO plays in the monitoring process. Your report has helped us sharpen our focus and increase our commitment to data security. Given the role that the NFC plays in the Department and in the Federal Government, it is absolutely essential that we not only have adequate security, but that we are among the best, if not the best, in either Government or the private sector for organizations carrying out similar functions. We intend to strengthen our information systems security program to meet the industry "best practices" standards as described in the May 1998 GAO report.

We welcome your continued advice and counsel to ensure this goal is met.

Sincerely,

FOR JOHN R. ORTEGO
Director

"An Equal Opportunity Employer"

GAO Contacts and Staff Acknowledgements

GAO Contacts

Carol A. Langelier, (202) 512-5079
Edward M. Glagola, Jr., (202) 512-6270
Lon C. Chin, (202) 512-2842

Acknowledgements

In addition to those named above, Debra M. Conner, Vernon L. Conyers, Jr., Shannon Q. Cross, Walter P. Opaska, and Christopher J. Warweg made key contributions to this report.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

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

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00