United States General Accounting Office

GAO

Report to the Mayor of the District of Columbia

January 2001

INFORMATION SECURITY

Weak Controls Place DC Highway Trust Fund and Other Data at Risk

GAO

Accountability * Integrity * Reliability

GAO-01-155

G A O
Accountability * Integrity * Reliability

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

January 31, 2001

The Honorable Anthony A. Williams
Mayor of the District of Columbia

Dear Mayor Williams:

We reviewed information system general controls[1] over the financial systems that process and account for the financial activities of the District of Columbia's Highway Trust Fund as part of our annual required audit of the Fund's financial statement for fiscal year 1999. Effective information system general controls are essential to ensure that Fund financial information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, and destruction.

This report discusses computer security weaknesses at (1) the Department of Public Works (DPW), which is responsible for processing, accounting for, and reporting on the Fund's financial activities and (2) the Office of the Chief Financial Officer (OCFO) and the Office of the Chief Technology Officer (OCTO), which are also responsible for information system general controls that could affect Fund financial systems. Because of the serious and pervasive nature of these weaknesses, we reported information system controls as a material weakness in the Fund's financial audit report for fiscal year 1999.[2]

Today, we are also issuing a report designated for "Limited Official Use," which describes each of the 50 computer security weaknesses identified in more detail and offers specific recommendations for correcting each of them. This version of the report provides a general summary of the weaknesses we identified and the recommendations we made. After we

[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.

[2]*Financial Audit: District of Columbia Highway Trust Fund's Fiscal Year Audit 1999 and 1998 Financial Statements* (GAO-01-41, October 31, 2000).

completed our fieldwork, the District provided us with information regarding corrective actions taken or planned. These actions are noted in this report; we intend to evaluate the effectiveness of these corrective actions as part of our follow-up on the District's implementation of our recommendations.

Results in Brief

Serious and pervasive computer security weaknesses place Fund and other District financial, payroll, personnel, and tax information at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction occurring without detection. These information system general control problems affected the District's ability to (1) prevent and/or detect unauthorized changes to Fund and other District financial information, including payroll and other payment data, (2) control electronic access to sensitive personnel and tax information, and (3) restrict physical access to sensitive computing areas. The computer security weaknesses we identified also increased the risk that financial and other sensitive information contained in District systems could be misused, fraudulently used, improperly disclosed, or destroyed, possibly without detection. Further, Fund and other District financial operations were vulnerable to disruption due to these weaknesses. Consequently, sensitive District personnel and tax information is at risk of disclosure, critical financial operations are at risk of disruption, and assets are at risk of loss.

Specifically, the District had not adequately limited access granted to authorized users, properly managed user IDs and passwords, effectively maintained system software controls, or sufficiently protected its networks and other computer systems from unauthorized users. The risks created by these access control weaknesses were compounded because the District was not routinely monitoring access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. In addition, the District was not providing adequate physical security for its computer facilities, appropriately segregating computer functions, properly controlling changes to application programs, or completely developing and testing disaster recovery plans.

A primary reason for the District's information system control problems was that it did not have a comprehensive computer security management program. 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 evaluating the effectiveness of established controls. Such a program, if

implemented effectively, would provide the District with a solid foundation for resolving existing computer security problems and managing its information security risks on an ongoing basis.

To improve information system general controls over Fund and other District financial operations, we are making recommendations to correct the computer security weaknesses we identified and to implement an entitywide computer security management program. District management stated that it has recognized the seriousness of the weaknesses we identified and expressed its commitment to improving information system controls.

In commenting on this report, the District concurred with our recommendations and said that it is giving the highest priority to correcting the information security weaknesses we identified. The District has developed an action plan to correct all security weaknesses by April 2002.

Background

In 1995, the District of Columbia established the Highway Trust Fund, as required by the District of Columbia Emergency Highway Relief Act.[3] This dedicated trust fund is required to include amounts equivalent to receipts from motor fuel taxes[4] and to be separate from the District's General Fund.[5] For fiscal year 1999, motor fuel tax revenues were reported to be almost $31 million.

[3]Public Law 104-21, 109 Stat. 257 (1995), D.C. Code Ann. Section 7-134.4 (2000 Supplement).

[4]The District of Columbia levies and collects a tax of 20 cents per gallon on motor vehicle fuels sold or otherwise disposed of within the District of Columbia by an importer or by a user or used for commercial purposes (D.C. Code Ann. Section 47-2301(1981, 1995 Replacement Vol.)).

[5]Unless prohibited by law (as in the case of the Fund under the act), the District's cash from all funds is combined into the General Fund's cash management pool, which is used to make transfers to all the District's checking accounts, as needed. Any cash not needed for immediate disbursement is invested.

The Fund is used to reimburse the District for local capital appropriated expenditures, which are (1) the District's share (normally 20 percent) of federal aid highway project costs, (2) the salaries of District personnel working directly on transportation capital projects, (3) overhead costs associated with federal aid projects, and (4) other nonparticipating costs.[6] All federal and local capital appropriated expenditures are paid out of DPW's Capital Operating account and then reimbursed by either the Department of Transportation's Federal Highway Administration (FHWA) or the Fund.

DPW is responsible for processing, accounting for, and reporting on the Fund's financial activities. To accomplish these functions, DPW relies on the System of Accounting and Reporting (SOAR), which is developed and maintained by OCFO. The District also uses SOAR to manage certain District-wide purchasing and financial reporting activities.

OCFO maintains SOAR, along with other District payroll, personnel, and tax information, on a computer system at its SHARE computer center. In fiscal year 1999, the District's two payroll and personnel applications—the Unified Pay and Personnel System and the Centralized Automated Payroll and Personnel System—accounted for more than $1.5 billion in reported expenditures relating to the District payroll and employee benefits. In addition, tax applications residing on this computer system controlled District sales and use, employer withholding, corporate franchise, unincorporated franchise and hotel, personal property, and individual income tax revenues for fiscal year 1999.

DPW also relies on its own local area network (LAN), the District's wide area network (WAN)—which is managed by OCTO—and the Internet to transfer Fund information to and from the SHARE computer center. The District's WAN not only allows DPW staff to access systems maintained at the SHARE computer center, but also connects other District organizations—such as the Metropolitan Police Department, the District General Hospital, and the District public school system—to these systems and systems at the District's other five data centers. In addition, some District financial information is maintained on the network. For example, the network-based Real Property Tax 2000 system contains land records,

[6]These include the District's expenditures for costs not eligible under the federal aid highway program, such as the costs for sewer cleaning, storm drain improvements, and retaining walls.

facilitates data analysis for property valuation and tax administration, maintains all District real property tax roll and levy entries, and supports automated management of real property tax accounts receivable adjustments, payment posting, and billing information. Altogether, the District's WAN serves about 30 sites, which support approximately 60 District agencies and offices.

To secure, protect, and preserve District information systems, such as those relied on to account for Fund and other District financial activities, District law requires the Mayor to establish, maintain, and provide consistent computer security policies, principles, and standards for all District departments and agencies.[7] More specifically, District law tasks OCTO with coordinating the development of information management plans, standards, systems, and procedures throughout the District government.[8]

Objective, Scope, and Methodology

Our objective was to evaluate the design and test the overall effectiveness of information system general controls over the Fund's financial systems, which are maintained and operated by three District organizations: DPW, OCFO, and OCTO. These information system general controls, however, also affect the security and reliability of other sensitive data, including District financial, payroll, personnel, and tax information, that is maintained on the same computer system as the Fund'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;
- assure recovery of computer processing operations in case of a disaster or other unexpected interruption; and

[7]March 15, 1985, D.C. Law 5-168, Section 4, 32 DCR 721; April 12, 1997, D.C. Law 11-259, Section 305(a), 44 DCR 1423; D.C. Code Section 1-1135, b, (6).

[8]March 26, 1999, D.C. Law 12-175, Section 1814, 45 DCR 7193; D.C. Code Section 1-1195.3 (4).

- ensure adequate computer security program management.

To evaluate these controls, we identified and reviewed District policies and procedures, conducted tests and observations of controls in operation, and held discussions with DPW, OCFO, and OCTO staff to determine if information system general controls were in place, adequately designed, and operating effectively. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual* (FISCAM),[9] which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data, and (2) the results of our May 1998 study of security management best practices at leading organizations,[10] which identifies key elements of an effective information security program.

We performed our work from June through August 2000 in accordance with generally accepted government auditing standards. Because the objective of our work was to assess the overall effectiveness of information system general controls, we did not fully evaluate all computer controls. Consequently, additional vulnerabilities could exist.

We requested comments on a draft of this report from the District's Chief Technology Officer. She provided us with written comments, which are discussed in the "Agency Comments" section and reprinted in appendix I.

Sensitive Data and Programs Were 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 the District's information system general controls found that they were not adequately protecting the Fund's financial activities or other District financial, payroll, personnel, and tax information that also reside at OCFO's SHARE computer center. Specifically, the District had not adequately limited access granted to authorized users, properly managed user IDs and passwords, effectively maintained system software controls, or sufficiently protected its networks and other computer systems from unauthorized

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

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

users. In addition, the risks created by these access control weaknesses were compounded because the District was not routinely monitoring access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. Consequently, District systems, programs, and data maintained at OCFO's SHARE computer center risk inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction occurring without detection.

District management has recognized the weaknesses we identified and has expressed its commitment to improving information system controls. Subsequent to our fieldwork, District officials provided us with action plans that, if implemented properly, should correct the weaknesses we identified. The following sections summarize the results of our review of information system general controls over the District financial systems used to manage Fund operations.

Access Authority Was Not Appropriately Limited for Authorized Users

A key weakness in the District's internal controls was that it was not adequately limiting the access of employees and other authorized users to Fund and other District financial, payroll, personnel, and tax information maintained at OCFO's SHARE computer center. Organizations can protect information from unauthorized changes or disclosures by granting employees authority to read or modify only those programs and data necessary to perform their duties. However, we found several examples where the District had not adequately restricted the access of legitimate users on the computer system that maintains Fund and other District financial, payroll, personnel, and tax information.

- The District allowed all of the more than 4,300 active user IDs full access to 20 system software libraries that are used 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 this system.
- Security software on the system that maintains Fund and other District financial, payroll, personnel, and tax information was not implemented to automatically deny unauthorized access attempts. We determined that 689 access rules controlling access to data and program files, including a system software library that could be used to bypass other security controls and a payroll library that contained check processing data, were set to generate a warning message when access violations occurred, but permit the unauthorized access to proceed. Consequently,

risk of improper access and changes to critical data files and programs occurring without detection is heightened.

- More than 265 user IDs on the system used to process Fund and other District financial information were granted the tape bypass label processing privilege that allows users to read and alter any tape regardless of other security software controls. These users included network support staff, database administrators, SOAR application programmers, payroll staff, Department of Human Services staff, and certain application users. As a result, these users have unlimited access to all tape files, including system audit logs and backup copies of sensitive financial and tax information.

One reason for the District's user access problems was that access authority was not being reviewed. Such reviews would have allowed the District to identify and correct inappropriate access.

OCFO officials told us that SHARE computer center staff had changed the security software configuration so that all unauthorized attempts are denied and restricted the tape bypass label processing privilege to only those users with a specific business need. OCFO officials also told us that SHARE computer center staff would complete reviewing and limiting access to sensitive system libraries by March 31, 2001. In addition, OCFO officials stated that procedures to periodically review (1) access granted to sensitive system files, (2) security software configuration settings, and (3) access activity allowed by the tape bypass label processing privilege for appropriateness would be implemented by March 31, 2001.

User ID and Password Management Controls Were Not Effective

In addition to overseeing user access authority, it is also 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 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 the effectiveness of these controls periodically to ensure that they are operating effectively.

At the District, however, user IDs and passwords were not being managed to sufficiently reduce the risk of unauthorized access to the computer

system that maintains Fund and other District financial, payroll, personnel, and tax information. For instance, the system was configured in a manner that did not always require passwords for user authentication. In addition, passwords that existed were not prevented from being (1) fewer than six characters, (2) the same as the user ID, or (3) other easily guessed words. Further, users were allowed the opportunity to circumvent password change requirements by reusing the same password over and over. Consequently, the District faced increased risks that passwords could be compromised to gain unauthorized access to financial and other sensitive information maintained on this computer system. OCFO officials told us that SHARE computer center staff had changed password control settings to require passwords to contain at least six characters and prevent passwords from being easily guessed words, such as the user ID.

We also found instances where the District was not promptly removing unused or unneeded IDs or deleting IDs for terminated employees. For example, more than 1,400 user IDs had not been used for at least 7 months. Allowing inactive IDs to persist poses needless risk that unnecessary IDs will be used to gain unauthorized access. We also found cases where terminated employees were provided the opportunity to sabotage or impair Fund and other District financial operations because their user IDs were not promptly disabled. OCFO officials told us that SHARE computer center staff would implement procedures to ensure that inactive IDs and IDs for terminated employees are promptly disabled no later than March 31, 2001.

System Software Controls Were Not Effective

It is also essential to control access to and modification of system software to protect the overall integrity and reliability of information systems. System software controls, which limit and monitor access to the powerful programs and sensitive files associated with computer system operation, 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, gain unauthorized privileges that allow improper actions, or circumvent edits and other controls built into application programs.

The District was not properly controlling system software to prevent access controls on the computer system used to process Fund and other District financial, payroll, and tax applications from being circumvented. The system software control weaknesses we identified diminish the reliability of financial and other sensitive information maintained on this

computer system and increase the risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and disruption.

In addition, we identified system software configuration weaknesses that could allow users to bypass access controls and gain unauthorized access to Fund and other District financial, payroll, personnel, and tax information. For example, the operating system was set up in a manner that allowed programs in any of the 74 libraries included in the normal search sequence[11] to perform sensitive system functions and operate outside of security software controls. Because users generally have access to such libraries, this greatly increases the risk that unauthorized programs could be introduced to bypass other access controls and improperly access or modify financial, audit trail, or other sensitive information maintained on this computer system.

Further, the District had not instituted processes to control changes to system software on this computer system. In the past 2 years, OCFO had implemented several major system software changes, such as installing new versions of database management, communication, access control, and operating system software. However, it was not maintaining a comprehensive log of system software changes, consistently documenting these changes and related test results, or independently testing system software changes before implementation. Consequently, the District faces increased risks of unintended operational problems caused by programming errors or the deliberate execution of unauthorized programs that could compromise security controls.

The District was also not adequately reviewing programs in sensitive system libraries to identify and correct weaknesses that could be used to circumvent security controls. Consequently, we found potential problems that, at a minimum, diminish the reliability of system software, but could also be exploited to introduce malicious code or circumvent other access controls. For example, 13 files capable of performing sensitive system privileges did not exist on the volume specified in the table used to manage such files. This increases the risk that unauthorized programs could be substituted for these files without management approval and used to bypass other security controls or inappropriately modify audit trails or sensitive data. Until the District begins actively managing programs in

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

sensitive system software libraries, it will not have adequate assurance that other security controls cannot be bypassed.

OCFO officials told us that SHARE computer center staff would implement policies and procedures by June 30, 2001, to (1) review system configuration settings periodically for appropriateness, (2) ensure that system software changes are authorized, independently tested, documented, and approved prior to implementation, and (3) evaluate programs in sensitive system libraries to identify and correct potential problems.

Network Security Was Not Sufficient

The risks associated with the access and system software control problems we identified were also heightened because the District was not adequately protecting access to its networks or restricting access to the system that processes Fund and other District financial applications from the Internet. We found several network user ID and password management weaknesses that could be exploited to gain unauthorized access to District systems. For example, a common default account was available on one DPW network server. In addition, certain network systems on the DPW LAN and/or District WAN were not set up to require password authentication, ensure that passwords were changed periodically, or disable user IDs after a specified number of invalid password attempts.

In addition, network system software configuration weaknesses could allow users to bypass access controls and gain unauthorized access to District networks or cause network system failures. For instance, certain network servers and routers were set up in a manner that permitted unauthorized users to connect to the network without entering valid user IDs and password combinations. This could allow unauthorized individuals to obtain access to system information describing the network environment, including user IDs, password properties, and account details.

These network security weaknesses not only increased the risk of unauthorized access to information maintained on the network, but also heightened the risk that intruders or authorized users with malicious intent could exploit the user ID and password management weaknesses described above to misuse, improperly disclose, or destroy Fund and other District financial and sensitive information.

DPW officials told us that they planned to correct the network ID, password, and system software configuration weaknesses we identified on the DPW LAN.

Access Activities Were Not Being Monitored

The risks created by the access control problems described above were also heightened significantly because the District was not adequately monitoring system and user activity. Such a program would include (1) network monitoring to promptly identify attempts by unauthorized users to gain access to District systems and (2) examining attempts to access sensitive information once entry to District systems is accomplished. Without these controls, the District has little assurance that improper attempts to access sensitive information would be detected in time to prevent or minimize damage.

The District organizations we visited had not implemented proactive network monitoring programs. Such a program would require the District to

- identify suspicious access patterns, such as repeated failed attempts to log-on to the network, attempts to identify systems and services on the network, connections to the network from unauthorized locations, and efforts to overload the network to disrupt operations, and
- implement intrusion detection systems to automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

The District had not installed intrusion detection software on its WAN. In addition, DPW was using available intrusion detection capabilities on only 2 of its 22 network segments. Further, a network server used to allow access through the Internet to the computer system that maintains Fund and other District financial and sensitive information was configured to not log any access activity.

DPW officials told us that they would review all network servers and activate intrusion detection capabilities on all servers with these capabilities. OCTO officials told us that in conjunction with their implementation of the District security management program planned for October 1, 2001, a central security group will be established that, among other things, will implement intrusion detection systems to identify suspicious access activities and notify appropriate agency personnel.

In addition, the District was not actively monitoring user access activity—to identify and investigate failed attempts to access sensitive data and resources or unusual patterns of successful access to such information—on the computer system used to process Fund and other District financial, payroll, personnel, and tax information. Routinely monitoring the access activities of authorized users, especially those who have the ability to alter sensitive programs and data, can help identify significant problems and deter users from inappropriate and unauthorized activities.

Because the volume of security information available is likely to be too voluminous to review routinely, the most effective monitoring efforts are those that selectively target specific actions. These monitoring efforts should include provisions to identify and investigate unusual or suspicious patterns of access, such as

- updates to security files that were not made by security staff,
- changes to sensitive system files that were not made by system programmers,
- modifications to production application programs that were not initiated by production control staff,
- revisions to production data that were completed by system or application programmers, and
- deviations from normal patterns of access to Fund and other District financial, payroll, personnel, and tax data.

The District could develop such a program by (1) identifying sensitive system files, programs, and data files on its computer systems and networks, (2) using the audit trail capabilities of its security software to document both failed and successful access to these resources, (3) defining normal patterns of access activity, (4) analyzing audit trail information to identify and report on access patterns that differ significantly from defined normal patterns, (5) investigating these potential security violations, and (6) taking appropriate action to discipline perpetrators, repair damage, and remedy the control weaknesses that allowed improper access to occur.

Although the District was maintaining a history log of access activity on the computer system that maintained Fund and other District financial information and was producing standard data set access violation reports, these reports were not targeted to specific actions and the District did not follow up to ensure that violations had been appropriately investigated. In addition, the District had not established a process to identify and investigate failed attempts to gain access to this computer system or

suspicious patterns of successful access to sensitive data and resources on this system.

OCFO officials told us that SHARE computer center staff had developed and tested programs to produce the types of targeted monitoring reports described above and plan to fully implement a program to routinely identify and investigate unusual or suspicious patterns of access to sensitive computer resources by March 31, 2001.

Other Information System Controls Were Not Sufficient

In addition to the access controls described above, there are other important information system general controls that organizations should have in place to ensure the integrity and reliability of data. These controls include policies, procedures, and control techniques to physically protect sensitive computer resources and information, provide appropriate segregation of duties among computer personnel, prevent unauthorized changes to application programs, and ensure the continuation of computer processing operations in case of unexpected interruption. We found weaknesses in each of these areas. The following sections summarize these weaknesses.

Physical Security Controls Were Not Effective

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 these resources are stored. In the District, 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.

However, we found weaknesses in physical security controls over computer systems at OCFO's SHARE computer center, which processes Fund and other District financial, payroll, personnel, and tax applications, and network servers connected to the DPW network. Neither DPW nor OCFO had developed formal procedures for granting and periodically reviewing access to the computer resources they controlled. As a result, staff could be granted access or continue to have access to sensitive network and system computer areas even though their job responsibilities may not warrant this access. For example, we identified 60 District employees and contractors who had been granted access to OCFO's SHARE computer center without evidence of formal authorization.

Likewise, DPW did not have complete or accurate records of which employees were permitted access to the network server room. In addition, OCFO staff could not account for 6 of the 95 cards that permitted access to the SHARE computer center computer room.

In addition, neither DPW nor OCFO was adequately controlling access by visitors, such as contractors, to sensitive computer areas. For example, we were able to enter and move about both DPW's network server room and OCFO's SHARE computer center, including sensitive areas, without providing identification, signing in, or being escorted. Consequently, employees or intruders with malicious intent might also be able to gain improper access to the SHARE computer center or DPW LAN and disrupt these operations.

In October 2000, DPW officials told us that they had corrected the physical security weaknesses we identified. In November 2000, OCFO officials told us that they had developed procedures for controlling access to the computer center.

Computer Duties Were Not Properly Segregated

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

The District had assigned incompatible duties to certain application and system programmers. For example, some of the 24 application programmers that developed computer programs for the District's main financial system, SOAR, were also responsible for supporting its operation. To perform these incompatible functions, certain application programmers were granted access to SOAR production programs and data. Further, the District had implemented access controls in a manner that permitted the remaining application programmers, who were not responsible for supporting SOAR operations, to also access SOAR production programs and data—a practice that violates basic segregation of duties principles. Allowing application programmers, especially those who have a detailed understanding of the application, to also modify SOAR production

programs and data increases the risk of unauthorized modifications, which could lead to improper payments.

In addition, all of the 13 system programmers responsible for maintaining the computer system that processes Fund and other District financial, payroll, personnel, and tax applications were also assigned certain incompatible functions. Some system programmers were also responsible for security administration, while others were also responsible for production control or database administration. Moreover, although each of the 13 system programmers was only responsible for certain incompatible functions, all of the 13 system programmers were granted access privileges that would allow them to also perform security administration, production control, and database administration functions. Allowing system programmers the capability to modify financial and other sensitive data and programs without any compensating controls increases the risks of unauthorized modification of financial information and inappropriate disclosure of sensitive data. In addition, because these individuals had both system and security administrator privileges, they had the ability to eliminate any evidence of their activity in the system.

Although District officials told us that they were aware of the potential problems associated with allowing incompatible computer duties to be performed by the same individual, the District had not implemented compensating controls, such as reviewing access activity, to mitigate increased risks. Until the District either restricts individuals from performing incompatible duties or implements compensating controls, Fund and other District financial and sensitive information will face increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection.

In November 2000, OCFO officials told us that they had limited the access of application programmers responsible for SOAR development to only read production programs and data. In addition, OCFO staff told us that system programming and security functions had been separated and that a special ID would be established to allow system programmers the access required to perform security functions. These activities would be logged and reviewed to ensure that only authorized activities are performed.

Changes to Application Programs Were Not Adequately Controlled

It is also 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 and program integrity, these changes should be documented, authorized, tested, independently reviewed, and implemented by a third party.

District policy did not require changes to its main financial system, SOAR, to (1) be approved or reviewed prior to implementation or (2) include guidelines for testing these changes. While SOAR application developers maintained a standardized change request form, these forms did not always include authorizing signatures or evidence of testing and independent review. For example, documentation for about 30 percent of the 26 changes that were made to correct problems with SOAR programs from October 1, 1999, through July 20, 2000, did not indicate that the change had been tested prior to implementation. In addition, documentation for almost 90 percent of these changes did not specify that an independent technical review had occurred. Further, the District had not established procedures for periodically reviewing SOAR programs to ensure that only authorized program changes had been implemented. Without adequate application change controls, the District faces increased risk that unauthorized or inadequately tested programs or modifications to existing programs could be introduced.

OCFO officials told us that policies and procedures to ensure that changes to SOAR programs are authorized, tested, independently reviewed, and approved would be implemented by January 2001. In addition, OCFO's policies will include a requirement to periodically review changes to SOAR programs to ensure that only authorized 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. 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 disaster.

None of the District organizations we visited had a complete and fully tested disaster recovery plan. For example, DPW had not developed a disaster recovery plan for its LAN. In addition, neither OCTO nor OCFO

had developed comprehensive disaster recovery plans for the District WAN or the SHARE computer center, which processes Fund and other District financial systems. Specifically, these OCTO and OCFO disaster recovery plans did not establish disaster recovery teams with specific roles and responsibilities, specify requirements for testing the plan periodically, or institute a process for reviewing and updating the plan based on test results. OCFO's disaster recovery plan for the SHARE computer center also did not address different types of risks, such as floods, winter storms, or interruptions in power or communications, that could affect the continuity of operations.

Furthermore, neither OCTO nor OCFO had fully tested disaster recovery plans for the District WAN or the SHARE computer center, respectively. OCFO did test the recovery of system software at its SHARE computer center in December 1999, but this test did not cover the center's critical applications or telecommunications. Until the District develops and fully tests comprehensive disaster recovery plans for the DPW LAN, the District WAN, and the SHARE computer center, it will not be assured that computer operations critical to the Fund and other District financial activities can be restored promptly in the event of a disaster or other unintended interruption.

OCFO officials told us that they had developed a disaster recovery plan for the SHARE computer center, which will use the District's Department of Human Resources' computer center. They stated that this plan will be fully implemented by June 30, 2001. In addition, DPW officials stated that their staff would develop a comprehensive disaster recovery plan for the DPW LAN by April 1, 2002.

Computer Security Management Program Was Not Adequate

A key reason for the District's information system control problems was that it did not have a comprehensive computer security management program in place to ensure that effective controls were established and maintained and that computer security received adequate attention. Our study of security management best practices found that leading organizations manage their information security risks through an ongoing cycle of activities coordinated by a central focal point.[12] This management process involves (1) assessing risk to determine computer security needs,

[12]GAO/AIMD-98-68.

(2) developing and implementing policies and controls that meet these needs, (3) promoting awareness to ensure that risks and responsibilities are understood, and (4) instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective. In contrast, the District had not adequately accomplished any of these objectives.

The first key problem with the District was that it had not adequately established a central focal point to coordinate computer security management. Due to the interconnectivity of the District's networks, coordination and guidance provided by a central focal point becomes even more important, since a compromise in a single system could impact all District agencies. According to District law, OCTO was created to (1) centralize responsibility for the District's information technology investments and (2) develop and enforce policy directives and standards regarding information technology throughout the District government. However, no single District office was overseeing the architecture, operations, configuration, or security of the District's networks and systems. For example, each of the District's five data centers remains responsible for operating and securing its own computer environment without sufficient District-wide guidance or oversight. In addition, while OCTO manages and secures the District WAN, other functional units, such as DPW, still manage their own networks. Consequently, security roles and responsibilities were not clearly assigned, security management was not given adequate attention, and no organization was held accountable for security throughout the District.

A second key area of computer security management is assessing risk to determine computer security needs. Risk assessments not only help management to determine which controls will most effectively mitigate risks, but also increase the awareness of risks and, thus, generate support for adopted policies and controls. In this regard, it is important for organizations to define a process, which can be adapted to different organizational units, to continually manage computer security risk. However, District policy did not require risk assessments or provide guidance for managing computer security risk on a continuing basis.

Consequently, none of the District organizations we visited were adequately managing risk relating to computer security, as evidenced by the serious weaknesses described above. For example, DPW had not performed a risk assessment for its network. In addition, OCTO had not formally assessed computer security risks relating to the District WAN,

which could affect all District agencies connected to this network. Further, OCFO was not routinely assessing and managing information security risks associated with its SHARE computer center, which processes Fund and other District financial, payroll, personnel, and tax systems. During the past year, the SHARE computer center had updated its computer hardware, upgraded its operating system software, and installed a new financial management system for the District. Although all of these events should have warranted a risk assessment, OCFO only performed an initial risk assessment for the new financial management system.

A third key element of effective security program management is implementing computer security policies and controls that cover all aspects of an organization's interconnected environment. Our study of security management practices at leading organizations found that current, comprehensive security policies, which cover all aspects of an organization's interconnected environment, are important because written policies are the primary mechanism by which management communicates its views and requirements.[13] We also reported that organizations should develop both high-level organizational policies, which emphasize fundamental requirements, and more detailed guidance or standards, which describe an approach for implementing policy.

Although District law tasks OCTO with coordinating the development of information management plans, standards, systems, and procedures throughout the District government,[14] OCTO had not yet established District-wide guidance for developing and implementing comprehensive computer security policies and controls. This, along with the fact that a central focal point had not been established to oversee computer security throughout the District, has contributed to unclear security roles and responsibilities. In one case, access to the District financial application had been removed for three terminated District employees, but access to the computer system that processes this and other District financial applications, which is maintained by another District organization, had not been disabled. Consequently these terminated employees still had the opportunity to sabotage or impair other District financial operations.

[13]GAO/AIMD-98-68.

[14]March 26, 1999, D.C. Law 12-175, Section 1814, 45 DCR 7193; D.C. Code Section 1-1195.3 (4).

In addition, the District had not developed technical standards for implementing security software, maintaining operating system integrity, or controlling sensitive utilities. Such standards would not only help ensure that appropriate information system controls were established consistently throughout the District, but also facilitate periodic reviews of these controls. The establishment of appropriate information system controls was also hindered because security administration and system programming staff were not provided with adequate technical training. Specifically, OCFO security administration staff at the SHARE computer center had not received security awareness training and had only been provided minimal training on the security software used by the District. In addition, OCFO system programmers at the SHARE computer center had not received technical training on important types of system software, such as the tape management system.

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.

However, none of the District organizations we visited were adequately promoting security awareness to ensure that such risks and responsibilities were understood. Several of the computer security weaknesses we discuss in this report indicate that users were either unaware of or insensitive to the need for important information system controls, such as secure passwords. We also found little evidence that the District had convinced its employees that it was important to prevent unauthorized access to the SHARE computer center and other sensitive computer areas. As discussed above, we were able to bypass physical security measures and enter and move freely about both OCFO's SHARE computer center and a DPW telecommunications room without detection or challenge.

A fifth key element of effective security management is an ongoing program of tests and evaluations to ensure that computer security policies and controls continue to be appropriate and effective. This type of

oversight is an essential aspect of security management because it (1) helps the organization take responsibility for its own security program and (2) can help identify and correct problems before they become major concerns. In addition, periodic assessments or reports on security activities can be a valuable means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security program.

Our study of security management best practices at leading organizations found that an effective control evaluation program includes processes for (1) monitoring compliance with established information system control policies and guidelines, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities.[15]

None of the District organizations we visited had established such a program, which could have allowed the District to identify and correct the types of weaknesses discussed in this report. Until the District establishes a program to periodically evaluate the effectiveness of information system controls, it will not be able to ensure that its computer systems and data are adequately protected from unauthorized access.

OCTO officials told us that they recognize the need for enhanced security and to this end, plan to implement a formal security management program by October 1, 2001. This program will include the key elements described in our study of security management best practices.

Conclusions

Information system general controls are critical to the District's ability to ensure the reliability of Fund and other District financial information and maintain the confidentiality of sensitive personnel and tax information. However, the District's information system control problems placed sensitive personnel and tax information at risk of disclosure, critical financial operations at risk of disruption, and assets at risk of loss.

A primary reason for the District's information system control problems is that it did not have a comprehensive security management program. Comprehensive computer security management programs are appropriate

[15]GAO/AIMD-98-68.

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 proactively 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.

District management stated that it has recognized the seriousness of the weaknesses we identified and expressed its commitment to improving information system controls.

Recommendations for Executive Action

We recommend that you direct the Chief Financial Officer, Chief Technology Officer, and the Director of DPW, as appropriate, to take the following actions.

- Correct the specific access control weaknesses which are summarized in this report and detailed, along with our corresponding recommendations and the District's corrective action plans, in a separate report designated for "Limited Official Use," also issued today.
- Report to you, or your designee, periodically on progress in implementing the corrective action plans described in the separate report designated for "Limited Official Use."

We also recommend that you direct the Chief Technology Officer to ensure that an effective entitywide security management program, as described in this report and in our study of security management best practices at leading organizations,[16] is developed and implemented. Such a program would include establishing a central focal point to manage an ongoing cycle of the following security management activities:

- assessing risk to determine computer security needs,
- developing and implementing policies and controls that meet these needs,
- promoting awareness to ensure that risks and responsibilities are understood, and

[16]GAO/AIMD-98-68.

- instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

Agency Comments

In commenting on a draft of this report, the District's Chief Technology Officer agreed with our findings and recommendations and stated that the District is giving the highest priority to correcting the information security weaknesses we identified. The District has developed an action plan to correct all security weaknesses by April 2002. Specifically, the District is making changes to its security software to reduce the risk of unauthorized access and to strengthen information system controls. In addition, the District plans to implement standard software and procedures across the appropriate computer platforms and to establish a team to address information security as part of normal business operations. OCTO also plans to conduct quarterly reviews to monitor the progress in implementing the corrective action plans associated with our recommendations.

The District also stated that it recognized that the key to information security is a sound security management program. By October 2001, with OCTO as the central focal point, the District plans to implement a security management program that will include conducting risk assessments, developing and implementing security policies and procedures, promoting awareness, and testing and evaluating controls to ensure that they are effective.

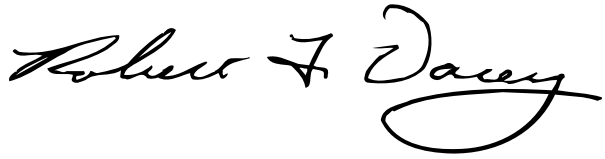
This report contains recommendations to you. The head of the District of Columbia Government is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations. You should send your statement to the Senate Committee on Governmental Affairs and the House Committee on Government Reform within 60 days of the date of this report. A written statement must also be sent to the House and Senate Committees on Appropriations with the District's first request for appropriations made more than 60 days after the date of this report.

We are sending copies of this report to Senator Robert C. Byrd, Senator Richard Durbin, Senator Kay Bailey Hutchison, Senator Joseph Lieberman, Senator Ted Stevens, Senator Fred Thompson, Representative Dan Burton, Representative Thomas M. Davis, Representative Ernest J. Istook, Representative James P. Moran, Representative Eleanor Holmes Norton, Representative David R. Obey, Representative Henry A. Waxman, and Representative C.W. Bill Young. We will also send copies to Kenneth R.

Wykle, Administrator of the Federal Highway Administration; Natwar Gandhi, Chief Financial Officer of the District of Columbia; Charles Maddox, Inspector General of the District of Columbia; Deborah K. Nichols, District of Columbia Auditor; Leslie Hotaling, Interim Director of the Department of Public Works; Suzanne Peck, Chief Technology Officer; and Alice Rivlin, Chairman of the District of Columbia Financial Responsibility and Management Assistance Authority.

If you have any questions or wish to discuss this report, please contact me at (202) 512-3317 or Dave Irvin at (214) 777-5716. Key contributors to this report are listed in appendix II.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

Comments From the District of Columbia

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

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

December 13, 2000

Joel C. Williamssen
Managing Director, Information Technology
United States General Accounting Office
Washington, D.C. 20548

RE: Response to GAO Draft Report "Information Security Weak Controls Place DC Highway Trust Fund and Other Data at Risk"

Dear Mr. Williamssen:

I am in receipt of your draft report entitled "Information Security – Weak Controls Place DC Highway Trust Fund and Other Data at Risk." As requested, I am providing comments on the General Accounting Office (GAO) recommendations found in the respective report. In summary, I am in agreement with the GAO findings and recommendations. Further, I want to assure you that the Department of Public Works (DPW), Office of the Chief Financial Officer (OCFO) and the Office of the Chief Technology Officer (OCTO) are giving the issues identified by GAO the most serious consideration and the highest priority, and a number of the appropriate remedies are identified below. My comments follow.

Correct the specific access control weaknesses GAO identified and summarized.

I appreciate GAO's diligence in pointing out where sensitive data and programs were vulnerable to unauthorized access, other information system controls were not sufficient and the computer security management program was not accurate. The appropriate changes are being made in the District's current security software by DPW, OCFO and OCTO to support GAO's recommendations on reducing risk to unauthorized access and strengthening information system controls. GAO also points out that an ongoing security management program needs to be implemented. This is an appropriate recommendation that can only be implemented after the addition of qualified personnel. OCTO is currently building the appropriate team to address information security as an ongoing program. The initial team should be in place in January of 2001 to insure that policies and procedures are implemented to review security exposures in the normal course of business. This will insure that security risks are identified and corrected as part of normal business operations. In addition, standard software and procedures will be implemented across the appropriate computing platforms so that a consistent, effective, and maintainable security program is administered. Please refer to the Responsibility Matrix, included as Attachment A, which indicates the agency responsible for addressing specific GAO findings and recommendations.

See comment 1.

441 4th Street, N.W., Washington, DC 20001 (202) 727-2277, Facsimile (202) 727-6857

Joel C. Williamssen
December 13, 2000
Page 2

Report periodically on the progress in implementing the corrective action plans recommended by GAO.

Quarterly, OCTO will review the progress in implementing the corrective action plans recommended by the GAO and will report the status to the City Administrator. The implementation dates provided in Attachment A will be closely monitored to insure the District is on target to achieving a sound information security program.

Develop and implement an effective entity-wide security management program.

The key to information security in the District is a sound security management program. Once key personnel are in place, OCTO will be the central focal point for developing an information security program which includes: security policies and procedures; segregation of critical functions; security training; security awareness; security monitoring and testing; management reporting; and risk assessment. The initial implementation of this program is planned for October 1, 2001 followed by appropriate tests and evaluations to insure that District security policies and controls are accurate and effective. With this program in place, I believe the District will have a sound basis for supporting the DC Highway Trust Fund.

Feel free to contact me at (202) 727-0839 or Cliff Brock, Director, District Data Centers, at (202) 727-5650.

Sincerely,

Suzanne J. Peck
Chief Technology Officer

cc: Natwar M. Gandhi, CFO
Anthony Pompa, OCFO
Pamela Graham, DPW

The following is GAO's comment on the District of Columbia's letter dated December 13, 2000.

GAO Comment

1. Attachment A is included only in our report designated for "Limited Official Use."

GAO Contact and Staff Acknowledgments

GAO Contact

Dave Irvin, (214) 777-5716

Acknowledgments

In addition to the person named above, Lon Chin, Debra Conner, Edward Glagola, David Hayes, Sharon Kittrell, Jeffrey Knott, West Coile, Harold Lewis, 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)**

PRINTED ON RECYCLED PAPER

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