

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL**

**FOLLOW-UP REVIEW OF
THE GENERAL ACCOUNTING OFFICE REPORT
CONCERNING THE DISTRICT OF COLUMBIA
HIGHWAY TRUST FUND
INFORMATION SECURITY**



**CHARLES C. MADDOX, ESQ.
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General



Inspector General

April 24, 2002

Suzanne J. Peck
Chief Technology Officer
Office of the Chief Technology Officer
441 Fourth Street, N.W., Suite 930S
Washington, D.C. 20001

Leslie Hotaling
Director
Department of Public Works
2000 14th Street, N.W. 6th Floor
Washington, D.C. 20009

Dear Ms. Peck and Ms. Hotaling:

Enclosed is our final report (OIG No. 02-1-1KA(a)) summarizing the results of the Office of the Inspector General's (OIG) follow up review of the recommendations made by the General Accounting Office (GAO) in their January 2001 report, "Weak Controls Place DC Highway Trust Fund and Other Data at Risk" (GAO-01-155). Our final report includes responses the Department of Public Works (DPW) and the Office of the Chief Technology Office (OCTO) made to the draft report.

The GAO report contained three findings, in which they summarized 10 information system control weaknesses. The 10 information system control weaknesses contained 50 computer security weaknesses that, if compromised, could affect the District's ability to prevent and/or detect unauthorized changes to the Fund and other District financial information. GAO made six recommendations for correcting each of the information system control weaknesses. Our audit identified an additional 21 computer security weaknesses, for a total of 71 specific computer security weaknesses requiring corrective actions by the DPW, OCTO, or both agencies. As of the date of this report, the District had taken corrective action on 36 computer security weaknesses and planned to take corrective actions on 31 computer security weaknesses. However, no action had been taken or planned for four computer security weaknesses.

The DPW concurred with our recommendations that concerned DPW and the District Division of Transportation and have initiated corrective actions.

In response to Recommendation 1, the OCTO indicated and provided supporting documentation that showed an additional 21 corrective actions were completed. Added to the 15 corrective actions completed at the time we issued the draft report, there are a total of 36 corrective actions taken to date. Corrective actions are in progress for 20 computer security weaknesses. OCTO had not taken corrective action on four computer security weaknesses. Additionally, OCTO did not respond by providing the current status on the in-process corrective action for 11 computer security weaknesses. OCTO believes that the Office of the Chief Financial Officer (OCFO) is responsible for the required corrective actions.

The OIG notes that the OCTO has made significant progress toward completing the corrective actions for information system control weaknesses, and agrees that the OCFO should respond to specific control weaknesses affecting its authority. However, the OIG believes that OCTO should be the repository for responses from OCFO. The OIG requests that OCTO provide the OIG with the results of the ongoing progress in implementing the outstanding 31 corrective actions associated with Recommendation 1.

The OCTO responded to our Recommendation 3 stating that the implementation of the new enterprise-wide Administrative Systems and Modernization Program (ASMP) will create a production environment and provide for separation of development and production responsibilities for human resources, general ledger, payroll and procurement through robust problem management, change management, production control, security processes and production. The OCTO stated that the ASMP should be implemented by the end of fiscal year 2004. The corrective actions planned for Recommendation 3 meet the intent of the recommendation.

The OCTO did not respond to Recommendations 2 and 4. We request that the OCTO revisit Recommendations 2 and 4 and provide comments within 30 days of the receipt of this report.

We appreciate the cooperation and courtesies extended to our staff during the audit. If you have any questions, please contact me or William J. DiVello, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,



Charles C. Maddox, Esq.
Inspector General

CCM/ws

Enclosure

DISTRIBUTION:

The Honorable Anthony A. Williams, Mayor, District of Columbia
Mr. Kelvin J. Robinson, Chief of Staff, Office of the Mayor
Mr. Tony Bullock, Interim Director, Office of Communications
The Honorable Linda W. Cropp, Chairman, Council of the District of Columbia
Ms. Phyllis Jones, Secretary to the Council (13 copies)
The Honorable Vincent B. Orange, Sr., Chairperson, Committee on Government Operations,
Council of the District of Columbia
Dr. Natwar M. Gandhi, Chief Financial Officer (4 copies)
Mr. Anthony F. Pompa, Deputy CFO for Financial Operations and Systems
Mr. Herbert J. Huff, Deputy Chief Financial Officer, Office of Tax and Revenue
Mr. Dan Tangherlini, Director, District Division of Transportation
Ms. Deborah K. Nichols, D.C. Auditor
Mr. Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO
Ms. Jeanette M. Franzel, Acting Director, Financial Management and Assurance, GAO
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives
Mr. Jon Bouker, Office of the Honorable Eleanor Holmes Norton
The Honorable Joe Knollenberg, Chairman, House Subcommittee on D.C. Appropriations
Mr. Jeff Onizuk, Legislative Director, House Subcommittee on D.C. Appropriations
Ms. Carol Murphy, Staff Assistant, House Subcommittee on D.C. Appropriations
The Honorable Chaka Fattah, House Committee on D. C. Appropriations
Mr. Tom Forhan, Minority Staff Director, Office of the Honorable Chaka Fattah
The Honorable Connie Morella, Chairman, House Subcommittee on D.C. Government Reform
Mr. Russell Smith, Staff Director, House Subcommittee on D.C. Government Reform
Mr. Mason Alinger, Professional Staff Member, Senate Subcommittee on D.C. Government
Oversight
The Honorable Richard Durbin, Chairman, Senate Subcommittee on D.C. Government
Oversight
Ms. Marianne Upton, Staff Director, Senate Subcommittee on D.C. Government Oversight
Ms. Kate Eltrich, Staff Director, Senate Subcommittee on D.C. Appropriations
Mr. Stan Skocki, Legislative Assistant, Senate Subcommittee on D.C. Appropriations
Mr. Charles Kieffer, Clerk, Senate Subcommittee on D.C. Appropriations

TABLE OF CONTENTS

	<u>PAGE</u>
EXECUTIVE DIGEST.....	1
INTRODUCTION.....	5
BACKGROUND	5
OBJECTIVE, SCOPE AND METHODOLOGY	5
FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS.....	6
REPORTED FINDING 1: SENSITIVE DATA AND PROGRAMS WERE VULNERABLE TO UNAUTHORIZED ACCESS (FIVE INFORMATION SYSTEM CONTROL WEAKNESSES).....	6
Control Weakness 1-1: Access Authority Was Not Appropriately Limited For Authorized Users.....	6
Control Weakness 1-2: User ID and Password Management Controls Were Not Effective	7
Control Weakness 1-3: System Software Controls Were Not Effective.....	8
Control Weakness 1-4: Network Security Was Insufficient	9
Control Weakness 1-5: Access Activities Were Not Monitored.....	9
REPORTED FINDING 2: OTHER INFORMATION SYSTEM CONTROLS WERE NOT SUFFICIENT (FOUR CONTROL WEAKNESSES).....	11
Control Weakness 2-1: Physical Security Controls Were Not Effective	11
Control Weakness 2-2: Computer Duties Were Not Properly Segregated	11
Control Weakness 2-3: Changes to Application Programs Were Not Adequately Controlled	12
Control Weakness 2-4: Service Continuity Planning Was Not Complete	12
REPORTED FINDING 3: COMPUTER SECURITY MANAGEMENT PROGRAM WAS NOT ADEQUATE (ONE CONTROL WEAKNESS).....	14
RECOMMENDATIONS.....	15
 EXHIBITS	
EXHIBIT A. OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES	15
EXHIBIT B. DPW MANAGEMENT RESPONSES TO DRAFT REPORT.....	21
EXHIBIT C. OCTO MANAGEMENT RESPONSES TO DRAFT REPORT.....	23

EXECUTIVE DIGEST

OVERVIEW

The Office of the Inspector General (OIG) is required by statute to conduct an annual financial statement audit of the Highway Trust Fund (Fund) and the accompanying 5-year Fund forecast. This audit was performed in conjunction with, and to facilitate, the audit of the Fund. The objective of our review was to determine the extent to which affected agencies have implemented and are complying with recommendations made by the General Accounting Office (GAO) in their January 2001 audit report, “Weak Controls Place DC Highway Trust Fund and Other Data at Risk” (GAO-01-155). The GAO audit focused on information system general controls over the financial systems that process and account for the financial activities of the District’s Fund.¹ This report summarizes the OIG’s follow-up review of the recommendations made by GAO.

Further, the report provides a summary of each of the reported GAO findings and recommendations along with references to Exhibit A, which contains specific computer security weaknesses, required corrective actions, and status. For example, the summary statement “The reported computer security weaknesses required one corrective action (1.A.1)”, refers the reader to the details provided in Exhibit A that are associated with GAO finding one, computer security weaknesses A, and the corresponding corrective action.

CONCLUSION

The GAO report contained 3 findings, which summarized 10 computer security weaknesses. The 10 computer security weaknesses contained 50 computer security weaknesses that, if compromised, could affect the District’s ability to prevent and/or detect unauthorized changes to the Fund and other District financial information. GAO made six recommendations for correcting each of the computer security weaknesses. In conducting our review, we identified 21 additional computer security weaknesses, which yielded a combined total of 71 specific computer security weaknesses requiring corrective actions by either the Department of Public Works (DPW), Office of the Chief Technology Officer (OCTO), or both agencies. A breakdown of the required 71 corrective actions by responsible agency is as follows:

- DPW corrective actions: 6
- OCTO corrective actions: 48
- BOTH corrective actions: 17

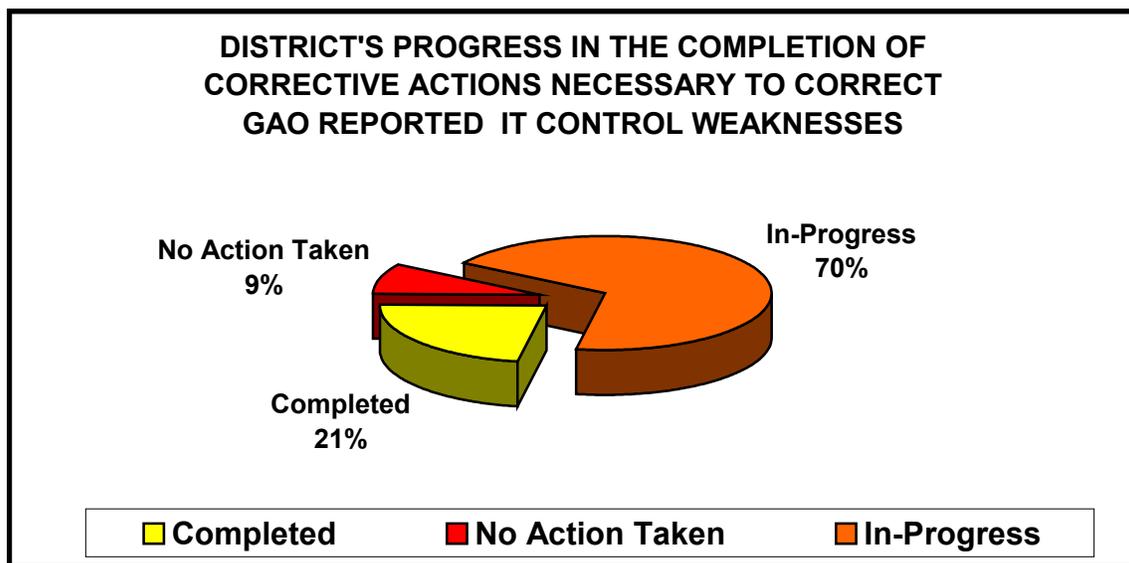
¹ Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical security protection designed to 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.

EXECUTIVE DIGEST

GAO reported that the District had developed an action plan to correct all computer security weaknesses by April 2002.

We found that as of October 2001, the District had completed 15 corrective actions and planned 50 corrective actions needed to address the GAO reported computer security weaknesses. However, no action had been taken or planned for six computer security weaknesses. A further breakdown of the progress of making the necessary corrective actions by responsible agency is depicted on the following page.

Shown below is the graphic presentation of the status of actions taken or planned to correct the computer security weaknesses reported by GAO.



Although corrective actions have been completed for 15 (21%) of the 71 computer security weaknesses, the District needs to take aggressive action to correct all of the GAO reported computer security weaknesses. Unless all of the corrective actions are implemented, we believe that serious and pervasive computer security weaknesses continue to place the Fund and other District financial, payroll, personnel, and tax information at risk of inadvertent or deliberate misuse.

CORRECTIVE ACTIONS

We addressed recommendations to DPW and OCTO that represent actions considered necessary to address the concerns described above. The recommendations, in part, center on:

EXECUTIVE DIGEST

- Completing corrective actions for the remaining 56 computer security weaknesses;
- notifying the OIG of the progress in implementing the corrective actions; and
- developing and implementing an entity-wide security management program.

MANAGEMENT COMMENTS

The DPW concurred with our recommendations that concerned DPW and the District Division of Transportation (DDOT) and have initiated corrective actions by: (1) filling a new Chief Technology/Information Officer position; (2) formulating a full disaster recovery plan; and (3) increasing the security of the DPW/DDOT network.

In response to recommendation 1, the OCTO indicated and provided supporting documentation that corrective actions were completed for 21 computer security weaknesses. Corrective actions are in progress for 20 computer security weaknesses, and four had no action taken. Additionally, the OCTO did not respond to 11 computer security weaknesses (1.B.5, 2.B.1-5, 2.B.7, 2.C.1, 2.B.3-5) because the OCTO believes that the Office of the Chief Financial Officer (OCFO) the OCFO is responsible for the required corrective actions.

The OCTO responded to our Recommendation 3 stating that the implementation of the new enterprise-wide Administrative Systems and Modernization Program (ASMP) will create a production environment and provide for separation of development and production responsibilities for human resources, general ledger, payroll and procurement through robust problem management, change management, production control, security processes and production. The OCTO stated that the ASMP should be implemented by the end of fiscal year 2004.

The OCTO did not respond to Recommendations 2 and 4.

OIG COMMENTS

The OIG believes that the actions taken by DPW are adequate and correct the identified computer security weaknesses. Since all identified computer security weaknesses have been corrected, we believe that DPW need not provide quarterly progress reports as required by Recommendation 2.

The OIG believes that the OCTO has made significant progress toward completing the corrective actions necessary to eliminate identified computer security weaknesses, and agrees that the OCFO should respond to specific control weaknesses affecting its authority. However, the OIG believes that OCTO should be the repository

EXECUTIVE DIGEST

for responses from OCFO. The OIG requests that OCTO provide the OIG with result of the ongoing progress in implementing outstanding corrective actions associated with Recommendation 1.

The corrective actions planned for Recommendation 3 to implement ASMP meet the intent of the recommendation and should correct the computer security weaknesses identified in our audit report.

We request that the OCTO revisit Recommendations 2 and 4 and provide comments within 30 days of the receipt of this report.

INTRODUCTION

BACKGROUND

Pursuant to D.C. Code, 2001 Ed. § 9-109.02(e), the OIG is required to perform the annual financial statement audit of the Fund. In conjunction with the financial statement audit of the Fund, the OIG conducted a follow-up review on recommendations made by the GAO in their January 2001 audit report, “Weak Controls Place DC Highway Trust Fund and Other Data at Risk” (GAO-01-155). The GAO report was the result of their assessment of the information system general controls over the Fund’s financial systems.

The Department of the Public Works (DPW) is responsible for processing, accounting for, and reporting on the Fund’s financial activities. Prior to October 2000, both the Office of the Chief Financial Officer (OCFO) and the Office of the Chief Technology Officer (OCTO) shared responsibility for information systems controls that could affect the Fund. However in October 2000, the OCFO transferred responsibility for managing the District’s SHARE Data Center to OCTO. The District’s SHARE Data Center currently known as ODC2 maintains the System of Accounting and Reporting (SOAR), along with the District’s personnel, payroll and tax information. DPW relies on SOAR, as well as their own local area network (LAN), the District’s wide area network (WAN), and the Internet for Fund information.

OBJECTIVE, SCOPE AND METHODOLOGY

The objective of our review was to determine whether the District has implemented agreed-to recommendations that were intended to correct the reported deficiencies as noted in the GAO report, and to determine the status of the recommendations that have not been corrected.

The scope of our review was limited to actions taken to address 10 computer security weaknesses identified by GAO. **(See Exhibit A)**. To accomplish our objectives, we conducted interviews and held discussions with District officials and the personnel responsible for taking corrective actions on each of the computer security weaknesses. Because of time constraints, we limited the scope of our work to a review and evaluation of documentation provided by District officials in support of corrective actions taken or planned on each of the computer security weaknesses. Our review was conducted in accordance with generally accepted auditing standards and included such tests as we considered necessary under the circumstances.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

REPORTED FINDING 1: SENSITIVE DATA AND PROGRAMS WERE VULNERABLE TO UNAUTHORIZED ACCESS (FIVE INFORMATION SYSTEM CONTROL WEAKNESSES)
--

Control Weakness 1-1: Access Authority Was Not Appropriately Limited For Authorized Users

GAO reported that the District had not adequately limited access authority of legitimate users and other authorized personnel from the District's financial systems. User access violations were not being properly reviewed, controlled, or limited, thereby increasing the risks that security controls could be bypassed or circumvented.

GAO recommended that OCTO:

- Review access to sensitive system libraries.² Limit access to those staff members who require it to perform their job functions. Develop and implement procedures for periodic review of dataset rules.³
- Operate ACF2⁴ in ABORT mode.⁵ Review dataset rules; eliminate the \$MODE⁶ (WARN) statement.⁷
- Remove the TAPEBLP privilege⁸ from all User IDs (UIDs)⁹ that do not have a regular need for it. Log and review all use of the TAPEBLP privilege.

The reported information system control weaknesses required four corrective actions (1.A.1 thru 1.A.4). We found that actions taken by OCTO to correct these computer security weaknesses were adequate.

² A library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area.

³ Data set rules are definition specifications that control inserting, replacing, and deleting data segments in logical relationships.

⁴ ACF-2 is a general security system that provides control over access to all resources under control of the operating system.

⁵ ABORT mode is the normal mode of operation that provides controlled termination of a processing activity when it cannot or should not continue.

⁶ \$MODE indicates the mode for this individual rule set. Used as a transition tool to ease the system in ABORT mode.

⁷ WARN is a security mode where access violations are logged and warning messages issued to enable processing to continue.

⁸ TAPEBLP is an attribute that allows users to access a tape data set without rule verification.

⁹ UID is a pointer to a character string containing the user ID and password, commonly the user identification, which is linked to a password providing a centralized access control mechanism that dictates individual user privileges.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

Control Weakness 1-2: User ID and Password Management Controls Were Not Effective

GAO reported that user IDs and passwords were not being properly managed to sufficiently reduce the risk of unauthorized access to the computer systems. They also identified instances where the system was configured in a manner that did not always require passwords for user authentication. Additionally, passwords existed that were: (1) fewer than six characters; (2) identical to the user's ID; or (3) easily discoverable words. GAO also reported that the District was not promptly removing unused, dormant or unneeded ID's or deleting ID's, for terminated employees.

GAO recommended that OCTO:

- develop and implement procedures for periodic review of Global Options.¹⁰
- set password options as follows: (1) PSWD REQUIRED=YES; 2) MIN PSWD LENGTH=8; (3) PSWD-LID=YES; (4) PSWD NUMERIC=YES, PSWD RESERVE WORD=YES; and (6) PSWD HISTORY=6.
- define to ACF-2 a list of passwords that should not be allowed.
- develop and implement procedures to:
 1. ensure that ODC2 security staff are notified immediately when a system user is terminated or no longer requires system access;¹¹
 2. verify periodically that all user access authorizations continue to be valid and that inactive accounts are disabled; and
 3. ensure that all user access authorizations are documented.

The reported computer security weaknesses required seven corrective actions to be taken by OCTO (1.B.1 - 1.B.7). We found that OCTO had only taken action to eliminate two computer security weaknesses (1.B.2-3). However, OCTO has initiated actions to eliminate the remaining five computer security weaknesses (1.B.1 and 1.B.4-7). These actions are scheduled for completion during the 1st quarter of calendar year 2002.

¹⁰ Global Options are features and options that determine system configuration settings or defaults.

¹¹ ODC2 is the former Share Data Center now known as OCTO Data Center Two. The Data center environment should provide adequate protection so that data (both programs and applications) are properly protected from unauthorized access, change, destruction, or misuse and that changes to data are properly controlled.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

Control Weakness 1-3: System Software Controls Were Not Effective

GAO reported that the District was not properly controlling system software to prevent access controls used to process the Trust Fund and other financial systems from being circumvented. Specifically, the District's system software configuration was set up in a manner that allowed users and programs to bypass access controls and gain unauthorized access to the computer system, perform sensitive system functions and operate outside of proper security controls. Additionally, there were no procedures to control changes to the software system or adequately review programs in sensitive system libraries that could be used to circumvent controls.

As a result, GAO recommended that OCTO:

- establish a warning banner.
- change the LNKAUTH¹² parameter from LNKAUTH=LNKLST to LNKAUTH=APFTAB.¹³
- define the level of access rules specific to each Authorized Programming Facility (APF) dataset name.
- review APF tables and the Link list and remove inappropriate entries.¹⁴
- develop and implement procedures for authorizing independent testing and approving system software changes.
- implement a targeted program to monitor access of sensitive program and files.
- develop and implement a process to periodically review programs in sensitive system software libraries.

The reported computer security weaknesses required seven corrective actions to be taken by OCTO (1.C.1 - 1.C.7). We found that OCTO had only taken action to eliminate one computer security weakness (1.C.1). However, our follow-up review disclosed that correction actions are in progress for five of the computer security weaknesses (1.C.2 - 1.C.6) and no action had been started for the remaining computer security weaknesses (1.C.7).

¹² LNKAUTH is a parameter that specifies whether the data sets in the Link List concatenation will be automatically APF authorized, or if they will only be authorized when they are also in the APF table defined by the PROGxx.ini configuration files. (PROGxx.ini contains the definition of the Authorized Program Facility (APF) table.

¹³ LNKAUTH=LNKLST or LNKAUTH=APFTAB establishes link listed libraries which are considered to be APF authorized by default and are required to be listed in the IEAAPFxx member(s). (IEAAPFxx this member controls the APF authorization of load libraries.

¹⁴ A Link List record defines one or more libraries that CA-ACF2 considers a logical extension to the system link list.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

Control Weakness 1-4: Network Security Was Insufficient

GAO cited several risks associated with network security access and system software controls and their inability to adequately protect and restrict access to the District's networks. GAO found several instances where network UID and password management controls could compromise the integrity of the District's financial systems. Additionally, the District had not securely configured computers and networks onto their existing network infrastructure to prevent unauthorized access. Finally, several network systems on the DPW LAN¹⁵ and DC WAN¹⁶ had not been set up to preclude password authentication, ensure periodic password changes or disable UIDs after a specified number of invalid password attempts.

GAO recommended that the following corrective actions be taken:

- evaluate user need for access and provide layers of controls to protect the network.
- require password change intervals every 30-90 days.
- change the "Null Session" setting.¹⁷

The reported computer security weaknesses required four corrective actions to be taken by DPW (1.D.1-1.D.4). We found that DPW completed corrective action on two computer security weaknesses (1.D.2 and 1.D.4) and initiated corrective actions for two computer security weaknesses (1.D.1 and 1.D.3).

Control Weakness 1-5: Access Activities Were Not Monitored

GAO noted that the District had not installed intrusion detection software on its WAN and had intrusion detection capabilities on only 2 of its 22 networks at DPW. In addition, a network server used to allow access through the Internet to the computer system had not been configured to log any access activity. GAO also concluded that the District was not actively monitoring user access activity, or investigating failed attempts to access sensitive data and information used to process the Fund and various District financial systems. Also, a history log of access activities was not targeted to specific actions and the District did not follow up to ensure that violations had been appropriately investigated.

¹⁵ Local Area Network (LAN) is a high-speed path between computers and associated equipment that provides resource, data, and program sharing or exchange within a limited geographical area.

¹⁶ Wide Area Network (WAN) is a type of formal communications network covering a wide geographical area.

¹⁷ Null session allows a hacker to obtain user, group, and share information without a valid username or password.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

GAO reported that the risks created by access control problems were significantly increased because of the inadequate systems monitoring and user activity procedures the District deployed. An effective monitoring program would ensure that: (1) mechanisms are in place to allow them to oversee normal activity, (2) the agency is alerted to unusual activity in a timely manner, and (3) security activity is logged and that any indication of an imminent security violation be promptly identified and acted upon in a timely manner. As a result, the District is at risk in its ability to adequately safeguard the information housed in the Districts financial system and detect all improper attempts to access the Fund's data.

GAO had no specific recommendation for this weakness; however, the OIG identified six corrective actions necessary to correct the reported computer security weaknesses related to this finding (1.E.1-1.E.6). Both OCTO and DPW have initiated corrective actions. Our review found that one corrective action had been completed (1.E.2) and that five were ongoing (1.E.1, 1.E.3-1.E.6).

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

REPORTED FINDING 2: OTHER INFORMATION SYSTEM CONTROLS WERE NOT SUFFICIENT (FOUR CONTROL WEAKNESSES)

Control Weakness 2-1: Physical Security Controls Were Not Effective

GAO noted that neither ODC2 nor DPW had developed formal procedures for granting and periodically reviewing access to the computer resources they housed. Additionally, GAO concluded that neither DPW nor the OCFO/OCTO was adequately controlling access by visitors, such as contractors, to sensitive system areas. Individuals were able to enter and move about both DPW's network server room and ODC2's sensitive system areas without restriction. According to the report, the District's physical access control measures, such as locks, badges, and alarms used to safeguard critical financial information and computer operations were inadequate.

GAO had no specific recommendation for this weakness; however, the OIG identified five corrective actions necessary to correct the reported computer security weaknesses related to this finding (2.A.1-2.A.5). Our review found that both DPW and OCTO have taken the necessary corrective actions to correct the reported computer security weaknesses.

Control Weakness 2-2: Computer Duties Were Not Properly Segregated

GAO reported that the District had assigned incompatible job responsibilities to certain application and system programmers. GAO noted 24 programmers who developed programs for the District's main financial system, SOAR, also supporting its operation. Moreover, certain application programmers with detailed knowledge of the SOAR application were permitted to modify SOAR production data. In addition, GAO showed evidence of system programmers, who were responsible only for certain incompatible functions, with access privileges that allowed them to perform security administration, production control, and database administration functions. Because of these capabilities, system programmers had the ability to modify the evidence of their activity on the system and make detection of such activity quite difficult.

GAO had no specific recommendation for this computer security weaknesses; however, the OIG identified seven corrective actions necessary to correct the reported computer security weaknesses related to this finding (2.B.1-2.B.7). Our review found that no corrective action had been completed. However, six of the corrective actions were in progress (2.B.1, 2.B.3-2.B.5), and one had not been acted upon (2.B.2).

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

Control Weakness 2-3: Changes to Application Programs Were Not Adequately Controlled

GAO noted that documentation for changes made to the financial system, SOAR, did not indicate that the changes had been tested prior to implementation. In addition, there was no evidence that an independent technical review had occurred regarding these changes. GAO also noted that the District had no established procedures for a periodic review of the SOAR programs to ensure that all changes were properly authorized. As a result, the District faced numerous risks that unauthorized or inadequately tested programs or modifications to existing programs could be introduced without detection.

GAO had no specific recommendation for this information system control weakness. However, in response to the GAO report, District officials stated that policies and procedures to ensure that changes to SOAR programs are authorized, tested, independently reviewed, and approved would be implemented by January 2001. As of the date of this report, these enhancements had not been implemented. Additionally, those policies would include a provision to periodically review changes to SOAR and ensure that only authorized changes are made.

The OIG identified five corrective actions necessary to correct the reported computer security weaknesses related to this finding (2.C.1-2.C.5). Our review found that OCTO had not taken any corrective actions to correct three computer security weaknesses (2.C.2-2.C.4). However, corrective actions were in progress for two of the computer security weaknesses (2.C.1 and 2.C.5).

Control Weakness 2-4: Service Continuity Planning Was Not Complete

GAO reported that none of the District organizations visited had a fully tested disaster recovery plan. Such plans should ensure that IT services are readily made available in the event of a major disruption. Without an adequate IT continuity framework, the District is at an increased risk for loss and damage to business operation activities in the event of a disaster.

GAO also noted that neither OCTO nor OCFO had developed comprehensive disaster recovery plans for the District WAN or the ODC2 computer center, which processes the Fund and other financial systems. Additionally, DPW had not developed a disaster recovery plan for its LAN. Specifically, OCTO and OCFO disaster recovery plans did not establish security teams with specific roles and responsibilities, or specify requirements for testing the plan or reviewing and updating the plan based on test results. GAO also pointed out that ODC2's disaster recovery plan did not address the different types of risks, such as floods, storms, or interruptions in power or communications, that could adversely affect the continuity of services.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

The GAO recommended that the following corrective actions be taken to correct these shortcomings:

- develop and implement a comprehensive disaster recovery plan.
- develop and implement interim procedures to minimize damage to the facility in the event of a fire.

In response, District officials stated that they had developed a disaster recovery plan for the ODC2 computer center, which will use the District's Department of Human Resources computer center. Additionally, ODC2 completed a preliminary risk assessment study in October 2001. They also stated that this plan would be fully implemented by June 30, 2001. As of the date of this report, neither OCTO nor OCFO had developed comprehensive disaster recovery plans for the District's financial systems. Also, DPW officials stated that they would develop a comprehensive disaster recovery plan for their LAN by April 1, 2002.

The OIG identified six corrective actions necessary to correct the reported computer security weaknesses related to this finding (2.D.1-2.D.6). Our review found that corrective actions were in progress for all six of the computer security weaknesses.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

REPORTED FINDING 3: COMPUTER SECURITY MANAGEMENT PROGRAM WAS NOT ADEQUATE (ONE CONTROL WEAKNESS)

GAO noted that the District had not established a central focal point to coordinate computer security matters or developed a comprehensive security management program. Specifically, each of the District's five data centers were operating and securing its own computer environment without District-wide guidance or oversight. For instance, OCTO manages and oversees the District's WAN, while DPW still manages their own internal network. Additionally, the framework for security roles and responsibilities were not clearly established or defined. This management framework involves: (1) assessing security risks to determine security needs; (2) developing and implementing policies and procedures that meet those needs; (3) promoting security awareness to ensure that risks and responsibilities are communicated and understood; (4) adjusting policies and procedures regularly and reevaluating periodically to ensure that policies and controls are appropriate and effective; (5) developing technical standards for implementing system software, maintaining the operating system integrity or controlling system utilities; and (6) establishing a program which would allow the District to identify and correct the types of weaknesses discussed in the report.

GAO also noted that access to the District's Financial application had been removed for three terminated employees, but access to the computer system that processes this and other financial applications had not been disabled. GAO concluded that none of the organizations they reviewed had adequately accomplished any of the above objectives and therefore made the following recommendations to OCTO:

- establish a central focal point to manage security.
- assess risk to determine computer security needs.
- develop and implement policies and controls that meet these needs.
- promote awareness to ensure that risk and responsibilities are understood.
- institute an ongoing program of test and evaluation to ensure that policies and procedures are appropriate and effective.

In response to GAO's report, OCTO stated that they recognized the need for enhanced security and planned to implement a formal security management program by October 1, 2001. This program is currently in draft form. OCTO also established the Director of IT Security position with a staff of 3 security officers and 11 contract support personnel. In order to be effective, this position should be highly visible and report directly to the Chief Technology Officer.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

The District has also taken the following actions in response to the GAO report:

- established a central focal point to manage security.
- assessed risk to determine computer security needs.
- developed and implemented policies and controls, currently in draft form, that meet these needs.
- scheduled and promote regular security awareness to ensure that risks and responsibilities are understood, with training scheduled to begin November 30, 2001.
- consolidated from five to three main data centers.
- implemented procedures governing sensitive data sets and libraries.

The OIG identified 20 corrective actions necessary to correct the reported computer security weaknesses related to this finding (3.1-3.20). Our review found that corrective actions were in progress for 19 of the computer security weaknesses (3.1-3.19), while no corrective action had been taken for one computer security weakness (3.20).

RECOMMENDATIONS

We recommend that the Department of Public Works and the Office of the Chief Technology Officer, as appropriate, take the following actions:

1. Complete the corrective actions for the 56 specific computer security weaknesses that are reported and detailed in Exhibit A, and
2. Notify the OIG quarterly on the progress in implementing the corrective action for each of the specific computer security weaknesses.

We are also repeating two specific recommendations that GAO made in their January 2001 report GAO-01-155, and also recommend that OCTO:

3. Ensure that an effective entity-wide security management program be developed and implemented, and
4. Institute an ongoing program of test and evaluation to ensure that policies and controls are appropriate and effective.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

DPW RESPONSE

The DPW concurred with our recommendations that concerned DPW and the DDOT and have initiated corrective actions by: (1) filling a new Chief Technology/Information Officer position; (2) formulating a full disaster recovery plan; and (3) increasing the security of the DPW/DDOT network.

OCTO RESPONSE

In response to recommendation 1, the OCTO indicated and provided supporting documentation that corrective actions were completed for 21 computer security weaknesses. Corrective actions are in progress for 20 computer security weaknesses, and four had no action taken. Additionally, the OCTO did not respond to 11 computer security weaknesses (1.B.5, 2.B.1-5, 2.B.7, 2.C.1, 2.B.3-5) because the OCTO believes that the Office of the Chief Financial Officer (OCFO) the OCFO is responsible for the required corrective actions.

The OCTO responded to our Recommendation 3 stating that the implementation of the new enterprise-wide Administrative Systems and Modernization Program (ASMP) will create a production environment and provide for separation of development and production responsibilities for human resources, general ledger, payroll and procurement through robust problem management, change management, production control, security processes and production. The OCTO stated that the ASMP should be implemented by the end of fiscal year 2004.

The OCTO did not respond to Recommendations 2 and 4.

OIG COMMENTS

The OIG believes that the actions taken by DPW are adequate and correct the identified computer security weaknesses. Since all identified computer security weaknesses have been corrected, we believe that DPW need not provide quarterly progress reports as required by Recommendation 2.

The OIG notes that the OCTO has made significant progress toward completing the corrective actions necessary to eliminate identified computer security weaknesses, and agrees that the OCFO should respond to specific control weaknesses affecting its authority. However, the OIG believes that OCTO should be the repository for responses from OCFO. The OIG requests that OCTO provide the OIG with result of the ongoing progress in implementing outstanding corrective actions associated with Recommendation 1.

FINDINGS AND FOLLOW-UP ON GAO RECOMMENDATIONS

The corrective actions planned for Recommendation 3 to implement ASMP meet the intent of the recommendation and should correct the computer security weaknesses identified in our audit report.

The OCTO did not respond to recommendations 2 and 4. We request that the OCTO revisit Recommendations 2 and 4 and provide comments within 15 days of the receipt of this report.

EXHIBITS

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report	OIG's Comments Regarding Implementation	Status	Responsible Agency(s)
1. Sensitive Data and Programs Were Vulnerable to Unauthorized Access			
1.A Access Authority Was Not Appropriately Limited For Authorized Users			
1	*4,300 active user IDs had full access to 20 sensitive system software libraries used to perform sensitive functions	Changed Authorized Programming File (APF) rules to restrict, update, and allocate to system and application programmer on a need to know basis only. Twenty UID have this capability. Procedures have been developed for granting access to sensitive system files. Data Center Manager to receive report when changes are made.	C OCTO
2	*security software was not implemented to deny unauthorized access attempts	ACF-2 rules changed to lock out users after 3 unsuccessful attempts. Privileged access restricted to 20 sys & certain app programmers on a need to know basis via APF rules.	C OCTO
3	*689 access rules could be used to bypass other security controls	DPW has firewall at each server. APF rules changed to limit privileged access to sys programmers on a need to know basis. ACF-2 rules now lock out users after 3 unsuccessful attempts. Removed the \$Mode (WARN) Statement. Changed ACF-2 rules to permanently operate in ABORT mode. Under this mode a command is sent to stop processing when unauthorized access is attempted.	C OCTO
4	*265 user IDs were granted the tape bypass label that allows users to read and alter any tape regardless of other security controls	TAPEBLP privilege removed from all UID and restricted to system programmers and certain production process UIDS based on need only. Data Center Manager reviews access semi annually or after changes are made. Procedures developed to support user request with foreign tapes.	C OCTO
1.B User ID and Password Management Controls Were Not Effective			
1	* user IDs and passwords were not being managed to sufficiently reduce the risk of unauthorized access to the computer system	ACF-2 enforces password history of 4 generations by default. Recommendation for 6 generation and 8 character passwords will be implemented on conversion to RACF. Currently, PSWD LENGTH = 6 set for password complexity.	I OCTO
2	*passwords existed where they were not prevented from being fewer than six characters long	ACF-2 rules changed to require minimum PSWD LENGTH = 6. All general user ID passwords required to expire within 30 days. Password control settings changed to require passwords to contain at least 6 characters. A daily report CSDAILY that includes environmental report ACFRPTNV is generated on all ACF-2 activity and accesses. There is currently a moratorium on major ACF-2 changes (exits).	C OCTO
3	* passwords that existed were not prevented from being the same as the user ID	Confirmed that the current system wide setting for ACF2 is set to disallow passwords from the same as the User ID. Control is now set to PSWD=LID=Yes . This rule disallows both the password and the User ID from being the same.	C OCTO
4	* passwords that existed were not prevented from being easily discoverable words	Recommendation for password complexity to be satisfied with conversion to RACF due 1st quarter of 2002.	I OCTO
5	* District was not promptly removing unused or unneeded IDs or deleting IDs for terminated employees	UID managers are contacted monthly by ODC2 regarding status of dormant UID. Procedure developed 7/16/01, Monthly logon ID maintenance Procedures. CS monthly developed and scheduled to run through CA7 Scheduler on the 20th day of each month.	I OCTO
6	* 1400 user IDs had not been used for at least 7 months	Developed Logon ID maintenance procedures. Reconcile monthly dormant UID by ODC2 with UID managers at agency level. Procedures developed 7/16/01. CS Monthly developed and scheduled to run through CA7 Scheduler.	I OCTO
7	* cases were terminated employees were provided opportunity to sabotage financial operations because user IDs were not promptly disabled	Daily activity reports generated on ACF-2 activity and accesses. This still could compromise financial data. Access should be granted on a need to know basis. In the meantime UID managers are contacted monthly regarding the status of dormant UIDs.	I OCTO

C - Action taken to correct the deficiency
 I - In process actions to correct deficiency
 N - No action taken to correct the deficiency

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report		OIG's Comments Regarding Implementation	Status	Responsible Agency(s)
I.C System Software Controls Were Not Effective				
1	* not properly controlling system software to prevent access controls on the computer system from being circumvented	System procedure manual is currently under development. A three phased approach to change APF Linklist. They now announce changes during weekly user meetings. Implemented LNKAUTH=LNKST to LNKAUTH=APFTAB in August 2001. Banner currently exists on dedicated terminal. Planned implementation on desktop in process. DCWAN Banner Page on OC-Web Connect.	C	OCTO
2	* identified system software configuration that could allow users to bypass access controls and gain unauthorized access	Procedures under development. Phased approach implemented in conjunction with previous item. Paper form updated to mainframe and physical access. Departmental email box established to receive electronic request. Provided read only access to all users by September 2001.	I	OCTO
3	* operating system was setup in a manner that allowed programs in any of 74 libraries included in a normal search sequence to perform sensitive system functions and operate outside of security controls	Security Officer will test list of rules and provide documentation to OIG. 3 phased approach implemented in conjunction with previous item. Implemented write access to system programmers only by September 2001.	I	OCTO
4	* had not instituted processes to control changes to system software on this computer system	Have a manual change control process in place. Reviewing a more robust procedure. Long term solution still under development. Changes are announced during user meetings	I	OCTO
5	* was not maintaining a comprehensive log of system software changes or consistently documenting these changes and test results	Under development will develop a comprehensive change control procedure. ENDEVOR software will be implemented in the 1st quarter of 2002.	I	OCTO
6	* 13 files capable of performing sensitive system privileges did not exist on the volume specified in the table used to manage such files	Have implemented SMS system to manage storage that tracks verifies and manages the enforcement rule of catalogued data sets. Specific logging records are collected nightly through batch job (ACFRPTDS) and redistributed to the Data Center Manager to review activity.	I	OCTO
7	* District was not adequately reviewing programs in sensitive system libraries to identify and correct weaknesses that could be used to circumvent security controls	Management will document by 3rd quarter 2002 policy to contain change by dividing task between individuals to address production control (CA-7 scheduler), change control, and disaster recovery. Endeavor will be implemented in the 1st quarter 2002.	N	OCTO
I.D Network Security Was Insufficient				
1	* several network user ID and password management weaknesses that could be exploited to gain unauthorized access	Implemented changes to force 90 day password changes. Developed DPW server account and password policies (changes 60 day interval).	I	DPW
2	* common default account was made available on one DPW network server	User accounts that had not been logged for 60 days are flagged. DPW removed common default accounts.	C	DPW
3	* certain network systems on the DPW LAN and/or District WAN were not set up to require password authorization, ensure passwords were changed periodically, or disable user IDs after a specified number of invalid password attempts	Five failed attempts to authenticate will lock user out, require password to be reset. DCWAN lock out after three unsuccessful attempts. Password change interval set at 30 days for DCWAN. DPW currently uses a 10 character requirement and force password changes to 60 days. DCWAN Banner page on OC-Web Connect.	I	OCTO/DPW
4	* 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	Null session allows one window server to logon remote windows server using a blank user name and password. DPW installed McAfee Software.	C	DPW
I.E Access Activities Were Not Monitored				
1	* District had not installed intrusion detection software on its WAN	In process of installing intrusion detection software on the DPW WAN and DC WAN. Director of Security had 4 intrusion detection demonstrations. Will later evaluate and determine which software to select and implement District-wide. (OCTO selected NFR Network Intrusion Detection (NFR NID) is an intrusion detection system.)	I	OCTO/DPW
2	* DPW was using available intrusion detection capabilities on only 2 of its 22 network segments	Active on all network segments. DPW currently monitoring network activity with Riversoft and Concord Software packages.	C	DPW

C - Action taken to correct the deficiency
I - In process actions to correct deficiency
N - No action taken to correct the deficiency

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report		OIG's Comments Regarding Implementation	Status	Responsible Agency(s)
3	* network server used to allow access through the Internet to the computer system that maintains District financial information	The District established a formal Information Security Program (currently in draft form) and created a Director of IT Security under OCTO. The security group is in the process of developing specific IT Security Policies and Procedures. OCTO plans to implement intrusion detection software on the DCWAN. DPW implemented McAfee virus detection software on all of its servers.	I	OCTO/DPW
4	* District was not actively monitoring user access activity to identify and investigate failed attempts to access sensitive data	Reviewing monthly security reports, monitoring account activities. DPW also monitors desk top Intel LANDESK application.	I	OCTO/DPW
5	* history log of access activity were not targeted to specific actions and the District did not follow up to ensure that violations had been appropriately investigated	Changed access rules at CDO2 to monitor account activities. DPW prints system logs for each of its servers weekly. Three failed assess attempts will lock user out requiring reset.	I	OCTO/DPW
6	* had not established a process to identify and investigate failed attempts to gain access to computer system	Set up firewall established login scripts that keep track of site activity. Installed forced password changes at regular intervals and monitor daily account activity. DPW prints system logs for each of its servers weekly. OCTO currently in process of developing specific IT Security Policies and Procedures.	I	OCTO/DPW
2. OTHER INFORMATION SYSTEM CONTROLS WERE NOT SUFFICIENT				
2.A Physical Security Controls Were Not Effective				
1	* Neither DPW nor OCFO had developed formal procedures for granting and periodically reviewing access to the computer resources	Established procedures requiring access by picture ID and escort of visitors. Paper forms updated for mainframe, and physical access at ODC2.	C	OCTO/DPW
2	* DPW did not have complete or accurate records of which employees were permitted access to the network server room	Updated ODC2, DPW and DC WAN entrance procedures, reporting to include photo IDs, card readers and name associated to cards.	C	OCTO/DPW
3	* 60 District employees and contractors who had been granted access to the OCFO's SHARE computer center without evidence of formal authorization	Performed a recertification of access. Implemented photo ID system in July 2001. Certification required by approval of Manager and set up with predefined expiration dates. Contractors are assigned to a 6 months maximum. Daily reports generated on ACF-2 activity and accesses.	C	OCTO/DPW
4	* OCFO staff could not account for 6 of the 95 cards that permitted access to the SHARE computer center computer room	Previous certification process cancelled. New entrance procedures were established. Completed August 2001. Old cards disabled, and all authorized users received new cards.	C	OCTO/DPW
5	* Neither DPW nor OCFO was adequately controlling access by visitors, such as contractors, to sensitive computer areas.	Implemented in conjunction with previous item. Established comprehensive entrance procedures affecting employees, visitors, contractors and sensitive computer areas. Both OCTO and DPW developed specific entrance procedures for DCWAN, DPW WAN, and ODC2.	C	OCTO/DPW
2.B Computer Duties Were Not Properly Segregated				
1	* had assigned incompatible duties to certain application and system programmers	Still have one user that has access to both categories (system and application programmer). Probably a staffing and training issue. These two functions should be separated. Management indicated that task will be divided between persons to address production control, change control and disaster recovery. Production ID and password control were identified and have been internally implemented to track the usage by application area.	I	OCTO
2	* 24 application programmers that developed computer programs for the Districts main financial system SOAR were also responsible for supporting its operation	Production control issue. ODC2 Data Center Manager stated that there is a lack of adequate staffing to support separated functions.	N	OCTO
3	* certain application programmers were granted access to SOAR production programs and data	In process of moving from distributed agency production to ODC2 CA 7 production scheduler. CA-7 will automate the schedule of production control.	I	OCTO

C - Action taken to correct the deficiency
 I - In process actions to correct deficiency
 N - No action taken to correct the deficiency

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report		OIG's Comments Regarding Implementation	Status	Responsible Agency(s)
4	* implemented controls in a manner that permitted application programmers, who were not responsible for supporting SOAR operations, to also access SOAR production programs and data	Duties documented to separated or divide function of production control, change control, disaster recovery, etc., change pilot project is planned.	I	OCTO
5	* all 13 programmers responsible for maintaining the computer system that processes financial data were also assigned certain incompatible functions	This will implemented in conjunction with previous item.	I	OCTO
6	* some system programmers were responsible for security administration, while others were also responsible for production control or database administration	Implemented in conjunction with previous item. CA-7 production scheduler will be handled at ODC2. CA-7 automates the scheduling and management of production workloads based on multiple levels of criteria dependencies, resource availability and time.	I	OCTO
7	* all of the 13 programmers were granted access privileges that would allow them to also perform security administration, production control, and database administration	This weaknesses will be implemented and corrected in conjunction with previous item. Division of task.	I	OCTO
2.C Changes to Application Programs Were Not Adequately Controlled				
1	* 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 changes	ODC2 Data Center Manager stated that policy and procedure would be developed in conjunction with the Endeavor change control software implementation. Endeavor is designed to streamline and automate complex software development process across the development life cycle to include software security, standard enforcement, change tracking and audit trails.	I	OCTO
2	* standardized change request forms did not always include authorizing signatures or evidence of testing and independent review	Open. Will be implemented in conjunction with previous item.	N	OCTO
3	* documentation for about 30% 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	Open	N	OCTO
4	* documentation for almost 90% of these changes did not specify that an independent technical review had occurred	Open	N	OCTO
5	* District had not established procedures for periodically reviewing SOAR programs to ensure authorized changes had been implemented	Will be implemented in conjunction with previous item.	I	OCTO
2.D Service Continuity Planning Was Not Complete				
1	* none of the District orgs visited had a complete and fully tested disaster recovery plan	A Risk Assessment analysis was performed by SUNGUARD. Will be implemented in conjunction with previous item. (Expected Completion Date: April, 2002) Have draft form of Disaster Recovery Plan. ODC2 estimates that it is about 50% complete. We concur. ODC2 has completed a preliminary risk assessment (SUNGUARD) study in October 2001. This will be the catalyst for a more comprehensive business continuity plan where ODC2 will be the recovery site for ODC1 and vise versa.	I	OCTO/DPW
2	* DPW had not developed a disaster recovery plan for its LAN	Data will be mirrored to the minute between ODC1 at Benning Road and ODC2 at Massachusetts Avenue data centers. Will be implemented in conjunction with previous item.	I	DPW
3	* Neither OCTO nor OCFO had developed comprehensive disaster recovery plans for the District WAN or the SHARE computer center	Will be implemented in conjunction with previous item. OCTO developed contingency plan for its WAN.	I	OCTO
4	* 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	Will be implemented in conjunction with previous item. Studying tape backup system and procedures.	I	OCTO

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report	OIG's Comments Regarding Implementation	Status	Responsible Agency(s)
5	* 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	Will be implemented in conjunction with previous item.	I OCTO
6	* OCTO nor OCFO had fully tested disaster recovery plans for the District WAN or the SHARE computer center	Will be implemented in conjunction with previous item.	I OCTO
3. Computer Security Management Program Was Not Adequate			
1	* had not adequately established a central focal point to coordinate computer security management	Created position description for Director of IT Security to include 3 Security Officer employees and 12 support contractors. This position should be a direct report to the Chief Technology Officer. OCTO also in the process of setting up Security Program. In order to be effective, the position of Director of IT Security should be highly visible and given appropriate responsibilities and authority. OCTO is in the process of setting up Security Program to address specific IT procedure.	I OCTO
2	* no single District office was overseeing the architecture operations, configuration, or security of the District networks and systems	Implemented in conjunction with previous item.	I OCTO/DPW
3	* each of the Districts five data centers remains responsible for operating and securing its own computer environment without sufficient District-wide guidance or oversight	District consolidated into 3 main data centers ODC1-Benning Road, ODC2 Mass. Avenue, and MPD. Common security policy will be District-wide.	I OCTO
4	* OCTO manages and secures the District WAN, other functional units, such as DPW, still manage their own networks	In process. Will be implemented in conjunction with establishment of comprehensive security policy	I OCTO/DPW
5	* security roles and responsibilities were not clearly assigned, security management as not given adequate attention, no organization was held accountable for security throughout the District	Established Policies and Procedures and Matrix chart in draft. Should be implemented in conjunction with establishment of comprehensive security policy.	I OCTO
6	* District policy did not require risk assessments or provide guidance for managing security risks on a continuing basis	Established Policies and Procedures in draft form. Regular awareness training will be scheduled and provided. Scheduled to begin November 30, 2001. Security awareness training started as scheduled.	I OCTO
7	* none of the District organizations visited were adequately managing risk relating to computer security	On an ongoing basis. Will be implemented in conjunction previous item.	I OCTO
8	* DPW had not performed a risk assessment for its network	Will be implemented and included with OCTO.	I OCTO/DPW
9	* OCTO had not formally assessed computer security risks relating to the District WAN which could affect all District agencies connected to this network	Concurrent ongoing development.	I OCTO
10	*OCFO was not routinely assessing and managing information security risks associated with its SHARE computer center.	ODC1 and ODC2 scheduled for this quarter.	I OCTO
11	* OCTO had not yet established District-wide guidance for developing and implementing comprehensive computer security policies and controls	DCWAN Concurrent ongoing development.	I OCTO
12	* central focal point had not been established to oversee computer security throughout the District, has contributed to unclear security roles and duties	Created position description and filled position, but not officially established for Director of IT Security, plus 3 full time Senior Security Managers and 12 contract support staff.	I OCTO
13	* access to District Financial applications had been removed for three terminated employees, but access to the computer system that processes this and other District financial applications, had not been disabled	A review of passwords revealed one user with access to financial data still had full access even though he transferred. Several users have multiple user Ids or duplicate UIDs.	I OCTO
14	* District had not developed technical standards for implementing security software, maintaining operating system integrity or controlling sensitive utilities	ODC2 has implemented procedures governing sensitive data sets and library access, but must be incorporated in overall District policy.	I OCTO

OVERVIEW AND ANALYSIS OF REPORTED INFORMATION TECHNOLOGY WEAKNESSES

Reported Weaknesses Made In The GAO Report	OIG's Comments Regarding Implementation	Status	Responsible Agency(s)	
15	* establishment of appropriate controls were hindered because security administration and system programming staff were not provided with adequate technical training	Open. ACF-2 issue, ODC2 indicated that this issue will be corrected when RACF is implemented.	I	OCTO
16	* OCFO security administration staff at the SHARE computer center had not received security awareness training and had only minimal training on security software used by the District	Security awareness training scheduled for November 30, 2001.	I	OCTO
17	* 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,	Open. ACF-2 issue, ODC2 indicated that this issue will be remedied when RACF is implemented.	I	OCTO
18	* none of District organizations visited were adequately promoting security awareness to ensure risks and responsibilities were understood	Regular awareness training will be scheduled and provided. Scheduled to begin November 30, 2001.	I	OCTO/DPW
19	* users were unaware of or insensitive to the need for important information system controls, such as a secure passwords	Should be promoted and will be implemented in conjunction with previous item.	I	OCTO/DPW
20	* none of the District organizations visited had established such a program, which would allow the District to identify and correct the types of weaknesses discussed in the report	Open. This is still a problem. No central focal point established for correcting control weaknesses identified in this report.	N	OCTO/DPW

C - Action taken to correct the deficiency
I - In process actions to correct deficiency
N - No action taken to correct the deficiency

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF PUBLIC WORKS



District Division of Transportation

March 29, 2001

Charles C. Maddox, Esq
Inspector General
717 14th Street, N. W.
Washington D. C. 20005

Dear Mr. Maddox:

This letter is in response to your draft audit of the Office of the Chief Technology Officer (OCTO) (OIG Report No. 02-1-1KA) and the Recommendations Follow-up Review to the GAO report issued previously.

As you know, OCTO was responsible for implementing most of the findings. However, in reviewing the report, several recommendations were also to include responses from the Department of Public Works (DPW) and District Division of Transportation (DDOT).

Those activities of concern to DPW and DDOT are as follows:

**Response to Control Weakness 2-4 - Service Continuity Planning was not complete.
Disaster recovery:**

Both DPW and DDOT recognized the lack of a disaster recovery plan and have since formulated a full disaster recovery plan. DPW and DDOT are going to utilize an existing contractor, IRON MOUNTAIN, for storing and rotating all backup tapes on a weekly basis. This contractor is currently used by OCTO's central data center for this purpose. As of now, DPW and DDOT are working on a Memorandum of Understanding with OCTO and a detailed "pick-up and drop-off plan" which is expected to be functioning by mid April, 2002. In addition, DPW and DDOT are exploring the full "hot site" option, where full off-site application support and remote systems access for users can be in place.

**Response to Control Weakness 1-4 - Network Security was Insufficient
Change the "null Session" setting:**

1.D-DPW/DDOT is currently operating with the following user ID password intervals:
routers-90 days
servers-90 days
NT user accounts-60 days
Novell user accounts-60 days

2000 14th Street, N.W., Washington, D.C. 20009 (202) 673-6813

Mail user accounts-60 days

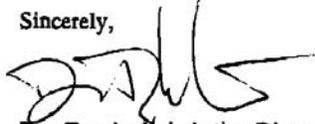
1-2.D-DPW/DDOT-currently user accounts are flagged to "disable" after no activity within a predetermined period of time; for DPW/DDOT's network that time is 60 days.

1-4.D-DPW/DDOT has restricted the access of any user or administrator from accessing any system platform, within DPW/DDOT's environment and under the control of the contractor operated SEAT Management Program, of "none password users accounts." Each time access is required, a user account and password is necessary to gain platform access.

DDOT has gone further than the specific recommendations made by the GAO. In order to both maintain the highest information technology standards and the needed security, DDOT has advertised and filled a new Chief Technology /Information Officer position.

Please let me know if you need any further assistance or clarification in this matter.

Sincerely,



Dan Tangherlini, Acting Director
District Division of Transportation

cc: Leslie Hotaling
Pamela Graham

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



March 7, 2002

Charles C. Maddox
Inspector General
Office of the Inspector General
717 14th Street, NW
Washington, DC 20005

Dear Mr. Maddox:

This letter is written in response to the draft report (OIG No. 02-1-1KA) summarizing your follow up review of the recommendations made by the General Accounting Office (GAO) in their January 2001 report, "Weak Controls Place DC Highway Trust Fund and Other Data at Risk" (GAO-01-155).

I've provided some general comments below, but the detailed responses to each audit item identified by The Office of the Inspector General (OIG) are provided in the detailed matrix and associated attachments enclosed with this letter. It appears that the OIG has listed audit items several times under different categories that were presented initially as one audit item in the GAO report. As a result, we've repeated our responses in a number of categories in an effort to comply with what we believe to be the intent of the OIG.

Many of the OIGs audit items center around a single, centralized issue – change and production control functions. OCTO cannot obtain additional Full Time Equivalent (FTE) positions to support these functions, and FTEs to support these functions are currently located in individual agency application development teams. Therefore, a management directive to move positions from the agencies to OCTO would have to be implemented to satisfy OIGs recommendation for centralized control over application change and production control functions.

In the initial GAO report detailed information was provided on system programs, system parameters, user identifications and passwords that GAO felt needed be added, deleted or modified. OCTO Data Center 2 (ODC2) addressed these specific items and developed procedures to ensure that system security functions would be maintained going forward. We believe these issues should be closed, as we've indicated in the detailed responses, unless the OIG has additional recommendations that ODC2 can address.

441 4th Street, N.W., Suite 930 South, Washington, DC 20001 Tel: (202) 727-2277 Fax: (202) 727-6857 Email: octo@dc.gov

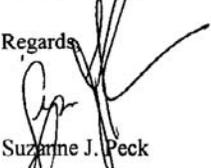
Charles C. Maddox
March 7, 2002
Page Two

The new, enterprise-wide Administrative Systems and Modernization Program (ASMP) will create a production environment and provide for separation of development and production responsibilities for human resources, general ledger, payroll and procurement through robust problem management, change management, production control, security processes and procedures. ASMP should be implemented by the end of fiscal 2004. Until then it will be extremely difficult to extract the system management functions from the development organization because none of the applications are completely documented.

Finally, the diagram attached as Figure 1 illustrates the division of responsibilities for DPW, the DCWAN and ODC2. No one organization has control or responsibility for the entire environment. DPW is responsible for applications, desktops, LAN hardware/software and security. OCTO DC WAN is responsible for availability, performance, capacity planning and security of the District-wide circuits, routers, switches and firewalls. OCTO ODC2 is responsible for operations, technical services and security of the payroll application for DPW. All other applications are the responsibility of DPW and processed in their environment.

If you have questions concerning this response or require further information, please contact me or Cliff Brock, Director, District Data Centers, at 727-5650.

Regards,

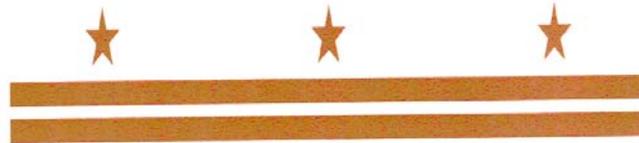


Suzanne J. Peck

Enclosures:

Figure 1 – Responsibility Diagram
Matrix of audit issues and OCTO responses
Attachment 1 – User Password Protection Procedure
Attachment 2 – Desktop Security Standard
Attachment 3 – Risk Management Program Document
Attachment 4 – Information Security Policy

cc: John Koskinen



District of Columbia
Office of the Chief Technology Officer
and
Office of the Chief Financial Officer

OIG Report No.02-1-1KA
Recommendations Follow-Up Review

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
1.A.1 4,300 active user IDs had full access to 20 sensitive system software libraries used to perform sensitive functions.	ODC2	Closed	Changed Authorized Programming File (APF) rules to restrict, update, and allocate to system and application programmer on a need to know basis only. Twenty UID have this capability. Procedures have been developed for granting access to sensitive system files. Data Center Manager to receive report when changes are made.
1.A.2 Security software was not implemented to deny unauthorized access attempts.	ODC2	Closed	ACF-2 rules changed to lock out users after 3 unsuccessful attempts. Privileged access restricted to 20 system programmers & certain applications programmers on a need to know basis via APF rules.
1.A.3 689 access rules could be used to bypass other security controls.	ODC2	Closed	DPW has firewall at each server. APF rules changed to limit privileged access to system programmers on a need to know basis. ACF-2 rules now lock out users after 3 unsuccessful attempts. Removed the \$Mode (WARN) Statement. Changed ACF-2 rules to permanently operate in ABORT mode. Under this mode a command is sent to stop processing when unauthorized access is attempted.
1.A.4 265 user IDs were granted the tape bypass label that allows users to read and alter any tape regardless of other security controls	ODC2	Closed	TAPEBLP privilege removed from all UID and restricted to system programmers and certain production process UIDS based on need only. Data Center Manager reviews access semi annually or after changes are made. Procedures developed to support user request with foreign tapes.
1.B.1 User IDs and passwords were not being managed to sufficiently reduce the risk of unauthorized access to the computer system	ODC2/Security	In-progress	ACF-2 enforces password history of 4 generations by default. Recommendation for 6 generation and 8 character passwords will be implemented on conversion to RACF. Currently, PSWD LENGTH = 6 set for password complexity. Expected completion date 4 th qtr 2002.
1.B.2 Passwords existed where they were not prevented from being fewer than six characters long.	ODC2	Closed	ACF-2 rules changed to require minimum PSWD LENGTH = 6. All general user ID passwords required to expire within 30 days. Password control settings changed to require passwords to contain at least 6 characters. A daily report CSDAILY that includes environmental report ACIRPTNV is generated on all ACF-2 activity and accesses. There is currently a moratorium on major ACF-2 changes (exits).
1.B.3 Passwords that existed were not prevented from being the same as the user ID	ODC2	Closed	Confirmed that the current system wide setting for ACF2 is set to disallow passwords from the same as the User ID. Control is now set to PSWD=I,ID=Yes. This rule disallows both the password and the User ID from being the same.
1.B.4 Passwords that existed were not prevented from being easily discoverable words.	ODC2	In-progress	Recommendation for password complexity to be satisfied with conversion to RACF due 4TH quarter of 2002.
1.B.5 District was not promptly removing unused or	ODC2	Closed for OCTO / In-	OCTO action sufficient since responsible managers are contacted monthly by the ODC2 security teams regarding the status of dormant user accounts. OCTO

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
unneded IDs or deleting IDs for terminated employees	Security	progress for OCTO	recognizes that the status of DC employees must come from a central source. During 2001 and 2002 ODC2 staff has requested receipt of a regular (daily) extract from the OCTO Payroll for the OCTO Data Centers to confirm the status of all active and terminated District employees. OCTO requests that the OCTO become responsible for this issue. Ultimately will be addressed with ASMP (Administrative Services Modernization Program - formerly ERP) system/relational database project that will have interfaces to data centers security.
I.C.1 Not properly controlling system software to prevent access controls on the computer system from being circumvented.	ODC2	Closed	OCTO requests detailed information on the issue. At present, there is not specific documentation from the IG to address this area. A three phased approach to change APF-Link list. They now announce changes during weekly user meetings. Implemented LNKAUTH=LNKST to LNKAUTH=APFTAB in August 2001. Banner currently exists on dedicated terminal. Planned implementation on desktop in process. DCWAN Banner Page on OC-Web Connect.
I. C.2 Identified system software configuration that could allow users to bypass access controls and gain unauthorized access.	ODC2	Closed	OCTO requests detailed information on the issue. At present, there is not specific documentation from the IG to address this area. OCTO believes this issue is closed and addressed in the response for item I.C.1.
I. C.3 Operating system was setup in a manner that allowed programs in any of 74 libraries included in a normal search sequence to perform sensitive system functions and operate outside of security controls.	ODC2	Closed	OCTO requests detailed information on this issue. At present, there is not specific documentation from the IG to address this area. OCTO believes this issue is closed and addressed in the response for item I.C.1.
I. C.4 Had not instituted processes to control changes to system software on this computer system.	OCTO	In-progress	A manual change control process is in place. Reviewing a more robust procedure. Long term solution still under development and involves implementation of REMEDY OCTO-wide (data centers & WAN) by January 2003. Changes are announced during user meetings. Change management will not be fully implemented until FY2003.
I. C.5 Was not maintaining a comprehensive log of system software changes or consistently documenting these changes and test results.	ODC2	In-progress	See OCTO response on finding I.C.4. Comprehensive change and configuration mgmt procedures under development.
I.C.6 13 files capable of performing sensitive system privileges did not exist on the volume specified in the table used to manage such files.	ODC2	Closed	OCTO requests detailed information on the issue. At present, there is not specific documentation from the IG to address this area. OCTO believes this issue is closed and addressed in the response for item I.C.1.

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
I.C.7 District was not adequately reviewing programs in sensitive system libraries to identify and correct weaknesses that could be used to circumvent security controls/	ODC2	Closed	OCTO requests detailed information on this issue. At present, there is not specific documentation from the IG to address this issue. Security Officer provided sensitive library access procedures (7/01) to OIG. A regular review process was identified within procedure. The Data Center Manager validated access levels for resources on 5/01 and again on 02/02. Additionally, specific logging records are collected nightly through batch job (ACTRPTDS) and maintained in SAR to perform daily review activity by Management.
I.D.1 Several network user ID and password management weaknesses that could be exploited to gain unauthorized access.	DPW	In-progress	Implemented changes to force 90 day password changes. Developed a DPW server account and password policies (changes 60 day interval). (See Attachment 1, "User Password Protection Procedure", for OCTO policy) Response needed from DPW.
I.D.2 Common default account was made available on one DPW network server.	DPW	Closed	User accounts that have not been logged for 60 days are flagged. DPW removed common default accounts.
I.D.3 Certain network systems on the DPW LAN and/or District WAN were not set up to require password authorization, ensure passwords were changed periodically, or disable user IDs after a specified number of invalid password attempts.	ODC2	In-progress	Five failed attempts to authenticate a password will lock the user out. It requires the password to be reset. DCWAN passwords lock out after three unsuccessful attempts. The password change interval is set at 30 days for DCWAN. DPW currently uses a 10 character requirement and force password changes to 60 days. DCWAN Banner page on OC-Web Connect.
	DC WAN	Closed	The WAN group does not manage the DPW network infrastructure. We only manage the dedicated link between them and the DCWAN.
	DPW		Response needed from DPW.
I.D.4 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.	DPW	Closed	A null session allows one window server to logon remote windows server using a blank user name and password. DPW installed McAfee Software
I.E.1 DPW was using available intrusion detection capabilities on only 2 of its 22 network	DPW	In-progress	Active on all network segments. DPW currently monitoring network activity with Riversoft and Concord Software packages. OCTO has selected Network Flight Recorder (NFR) as the Enterprise Intrusion Detection System (IDS).

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
segments.			Implementation on DC WAN is in progress, expected completion date is April 2002. IDS will monitor DC WAN network activity at critical sites including DPW. Response needed from DPW.
1.E.2 Network server used to allow access through the Internet to the computer system that maintains District financial information.	Security/DPW	Closed	The District established a formal Information Security Program (currently in draft form) and created a Director of IT Security under OCTO. The security group is in the process of developing specific IT Security Policies and Procedures. OCTO plans to implement intrusion detection software on the DCWAN. DPW implemented McAfee virus detection software on all of its servers.
1.E.3 Network server used to allow access through the Internet to the computer system that maintains District financial information.	Security	In-progress	The District established a formal Information Security Program (currently in draft form) and created a Director of IT Security under OCTO. The security group is in the process of developing specific IT Security Policies and Procedures. OCTO plans to implement intrusion detection software on the DCWAN. DPW implemented McAfee virus detection software on all of its servers.
1.E.4 District was not actively monitoring user access activity to identify and investigate failed attempts to access sensitive data.	DPW	In-progress	Reviewing monthly security reports, monitoring account activities. DPW also monitors desk top Intel LANDISK application. Response needed from DPW.
1.E.5 History log of access activity were not targeted to specific actions and the District did not follow up to ensure that violations had been appropriately investigated.	DPW	In-progress	Changed access rules at ODC2 to monitor account activities. DPW prints system logs for each of its servers weekly. Three failed access attempts will lock the user out requiring a password reset. Response needed from DPW.
1.E.6 Had not established a process to identify and investigate failed attempts to gain access to computer system.	Security DPW	Closed	Set up firewall and established login scripts that keep track of the site activity. Installed forced password changes at regular intervals and monitor daily account activity. DPW prints system logs for each of its servers weekly. OCTO is currently in the process of developing specific IT Security Policies and Procedures. (See Attachment 2, "Desktop Security Standard", for OCTO policy.) Response needed from DPW.
2.A.1 Neither DPW nor OCTO had developed formal procedures for granting and periodically reviewing access to the computer resources.	ODC2 DPW	Closed	Procedures were established requiring access by picture ID and escort of visitors. Paper forms are updated for mainframe, and physical access at ODC2. Response needed from DPW

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
2.A.2 DPW did not have complete or accurate records of which employees were permitted access to the network server room.	ODC2/DC WAN DPW	Closed	Updated ODC2, DPW, and DC WAN entrance procedures, reporting to include photo IDs, card readers and name associated to cards. Response needed from DPW.
2.A.3 60 District employees and contractors who had been granted access to the OCFO's SHARE computer center without evidence of formal authorization.	ODC2	Closed	Performed a review of access. Implemented photo ID system in July 2001. Certification is required by approval of Manager and set up with predefined expiration dates. Contractors are assigned to a 6 months maximum. Daily reports generated on ACT-2 activity and accesses.
2.A.4 OCFO staff could not account for 6 of the 95 cards that permitted access to the SHARE computer center computer room	ODC2	Closed	Previous certification process was cancelled. New entrance procedures have been established. (Completed August 2001.) Old cards have been disabled and all authorized users received new cards.
2.A.5 Neither DPW nor OCFO was adequately controlling access by visitors, such as contractors, to sensitive computer areas.	ODC2	Closed	Implemented in conjunction with previous item. Established a comprehensive entrance procedure affecting employees, visitors, contractors and sensitive computer areas. Both OCFO and DPW developed specific entrance procedures for DCWAN, DPW LAN, and ODC2.
2.B.1 Had assigned incompatible duties to certain application and system programmers.	ODC2 OCFO	In-progress	There is one agency that continues to have access to both systems and applications. These two functions will be separated to address production control change control and disaster recovery. Production ID and password control are identified and being tracked. This issue needs OCFO response.
2.B.2 24 application programmers that developed computer programs for the Districts main financial system SOAR were also responsible for supporting its operation.	ODC2 OCFO	No action taken	Due to a production control issue, ODC2 Data Center Manager stated that there is a lack of adequate staffing to support separated functions. This issue needs OCFO response.
2.B.3 Certain application programmers were granted access to SOAR production programs and data.	ODC2 OCFO	In-progress	ODC2 is currently in the process of moving from a distributed agency production to ODC2 CA-7 production scheduler. CA-7 will automate the schedule of production control. OCFO has CA-7. OCFO does not manage applications software for agencies.

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
			This issue needs OCFO response.
2.B.4 Implemented controls in a manner that permitted application programmers, who were not responsible for supporting SOAR operations, to also access SOAR production programs and data.	ODC2 OCFO	In-progress	Duties are documented to separate or divide functions of production control, change control, disaster recovery, etc. A change pilot project is planned. Documentation for production control has been initiated. This issue needs OCFO response.
2.B.5 All 13 programmers responsible for maintaining the computer system that processes financial data were also assigned certain incompatible functions.	ODC2 OCFO	In-progress	This will be implemented in conjunction with previous item. This issue needs OCFO response.
2.B.6 Some system programmers were responsible for security administration, while others were also responsible for production control or database administration.	ODC2	In-progress	OCFO requests detailed information on the issue. At present, there is not specific documentation from the IG to address this area. Action to be implemented in conjunction with item 2.B.4. Some production scheduling is handled at ODC2. CA-7 automates the scheduling and management of production workloads based on multiple levels of criteria dependencies, resource availability, and time. ODC2 systems programmers do not have security administration authority, but do require system administrator access to databases which is compliant with separation of duties.
2.B.7 All of the 13 programmers were granted access privileges that would allow them to also perform security administration, production control, and database administration.	ODC2 OCFO	In-progress	These weaknesses will be implemented and corrected in conjunction with previous item, division of tasks. This issue needs OCFO response.
2.C.1 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 changes	ODC2 OCFO	In-progress	ODC2 Data Center Director stated that policy and procedure would be developed in conjunction with ENDEVOR. It is designed to streamline and automate complex software development process across the development life cycle to include software security, standard enforcement, change tracking, and audit trails. This issue needs OCFO response.
2.C.2 Standardized change request forms did not always include authorizing signatures or evidence of testing and independent review.	DC WAN	In-progress	The Configuration/Change Control Board has been chartered. Changes are reviewed and approved weekly. The test lab is operational.
2.C.3 Documentation for about 30% of the 26 changes that were made to correct problems with SOAR	OCFO	No action taken	This issue needs OCFO response.

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
programs from October 1, 1999, through July 20, 2000, did not indicate that the change had been tested prior to implementation.			
2.C.4 documentation for almost 90% of these changes did not specify that an independent technical review had occurred	OCFO	No action taken	This issue needs OCFO response.
2.C.5 District had not established procedures for periodically reviewing SOAR programs to ensure authorized changes had been implemented	OCFO	In-progress	This issue needs OCFO response.
2.D.1 None of the District orgs visited had a complete and fully tested disaster recovery plan.	ODC2	In-progress	A Disaster Recovery Plan exists in draft form. ODC2 estimates that it is about 20% complete. A Risk Assessment analysis was performed by SUNGUARD on 10/01, and will be the catalyst for a more comprehensive business continuity plan where ODC2 and ODC1 will serve as backup recovery sites to each other. Implementation of Disaster Recovery Plan is first quarter of 2003.
2.D.2 DPW had not developed a disaster recovery plan for its LAN	DPW	In-progress	This issue needs DPW response.
2.D.3 Neither OCTO nor OCFO had developed comprehensive disaster recovery plans for the District WAN or the SHARE computer center.	ODC2	In-progress	ODC2 (SHARE) plans will be implemented in conjunction with item 2.D.1.
2.D.4 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	ODC2	In-progress	Will be implemented in conjunction with item 2.D.1. Studying tape backup system and procedures.
2.D.5 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	ODC2	In-progress	A risk assessment analysis was performed by SUNGUARD on 10/01, and will be used for a more comprehensive Disaster Recovery plan for the District's Data Centers. An enterprise Tape Storage system and redundant Network Operations Centers are being implemented this year to support the Disaster Recovery process.
2.D.6	ODC2	In-progress	Will be implemented in conjunction with item 2.D.1.

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
OCTO nor OCFO had fully tested disaster recovery plans for the District WAN or the SHARE computer center	DCWAN	In-progress	OCTO is in the process of building two redundant Data Centers. One at 3919 Benning Rd. (ODC1), which was chosen as the new primary core site because of future mainframe consolidation, data traffic flow, adequate space, and secure facilities. The backup core site is located at 222 Mass Ave. (ODC2/Share). The goal is to relocate the internet point of presence, firewall, DMZ, core routers and switches, and some mission-critical servers both at ODC1 and ODC2. Mission-critical servers, intranet servers, DNS, and email servers will be installed and configured to provide redundancy between both core Data Centers. This was designed primarily to support Disaster Recovery.
3.1 Had not adequately established a central focal point to coordinate computer security management.	Security	Closed	Created a position description for Director of IT Security to include 3 Security Officer employees and 12 support contractors. This position should be a direct report to the Chief Technology Officer. OCTO is also in the process of setting up Security Program. In order to be effective, the position of Director of IT Security should be highly visible and given appropriate responsibilities and authority. OCTO is in the process of setting up a Security Program to address specific IT procedures. A District of Columbia Information Technology Security Program has been established and is operational. A Director of IT Security position has been created. This program under the Director is responsible for providing District-wide oversight, guidance, and accountability for IT security. This organization serves as the focal point for IT security within the District.
3.2 No single District office was overseeing the architecture operations, configuration, or security of the District networks and systems.	Security	Closed	Implemented in conjunction with the previous item. A District of Columbia Information Technology Security program has been established and is operational. This program under the Director is responsible for providing District-wide oversight, guidance, and accountability for IT security. This organization serves as the focal point for IT security within the District.
3.3 Each of the Districts five data centers remains responsible for operating and securing its own computer environment without sufficient District-wide guidance or oversight.	Security	Closed	The District was consolidated into 3 main data centers ODC1-Benning Road, ODC2 Mass. Avenue, and MPD. Common security policy will be District-wide. RACF is being implemented as the standard mainframe security package across all data centers.
3.4 OCTO manages and secures the District WAN, other functional units, such as DPW, still manage their own networks.	Security DPW	In-progress Pending	Will be implemented in conjunction with establishment of OCTO policy. Response needed from DPW.

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
			was developed. Monthly meetings have been held since August 2001, during which the risks inherent to OCTO operations were identified, ranked according to the criteria required by the DC Office of Risk Management, and the most critical are being addressed as budgets allow. The progress of risk abatement is reviewed monthly. The Risk Management Program that OCTO submitted to the Office of Risk Management, and is following, is attached. (See Attachment 3, "Risk Management Program")
3.7 None of the District organizations visited adequately managing risk relating to computer security.	Security	In-progress	Risk assessments are evaluated on an ongoing basis. Will be implemented in conjunction previous item. Agencies need to coordinate with DC RACC Risk Management Program.
	RACC	In-progress	See response from 3.6
3.8 DPW had not performed a risk assessment for its network	Security	In-progress	Will be implemented and included with OCTO. DPW is scheduled to have a security assessment completed in March 2002.
3.9 OCTO had not formally assessed computer security risks relating to the District WAN which could affect all District agencies connected to this network.	Security	In-progress	Concurrent with response in 3.7, ongoing and in development. OCTO is scheduled to have the District WAN assessment completed in March 2002.
	DCWAN	Closed	OCTO has been responsible in the past to standardize desktop and security features. Any new standards or procedures are being handled by the security group.
3.10 OCFO was not routinely assessing and managing information security risks associated with its SHARE computer center.	Security	In-progress	Data Center's (ODC1&ODC2) information security risk and vulnerability assessments planned for 2002. They have not yet contracted.
3.11 OCTO had not yet established District-wide guidance for developing and implementing comprehensive computer security policies and controls	Security	Closed	OCTO has established and implemented District-wide security guidance and policies, in addition to ongoing awareness and training.
3.12 Central focal point had not been established to oversee computer security throughout the District, has contributed to unclear security roles and duties.	Security	Closed	Director of IT Security position has been created. This position is responsible for providing District-wide oversight, guidance, and accountability for IT security. This individual is in charge of the organization that serves as the focal point for IT security within the District.
3.13 Access to District Financial applications had	ODC2	Closed	OCTO requests detailed information on the issue. At present, there is not specific documentation from the IG to address this area. OCTO believes this

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
been removed for three terminated employees, but access to the computer system that processes this and other District financial applications, had not been disabled.			issue is closed and addressed in the response for item 1.B.5.
3.14 District had not developed technical standards for implementing security software, maintaining operating system integrity or controlling sensitive utilities.	ODC2	In-progress	ODC2 has implemented procedures governing sensitive data sets and library access. Reviewing OCTO Software management policy to incorporate change and configuration guidelines. Contracted JH Technologies to complete a project that identifies comprehensive technical standards (ITIL) and produce a prioritized work plan by March 2002.
3.15 Establishment of appropriate controls were hindered because security administration and system programming staff were not provided with adequate technical training.	ODC2/Security	Closed	ODC2 security staff received comprehensive training on ACI-2 administration and will also receive training on new products as required. This issue will be corrected when RACF is implemented.
3.16 OCTO security administration staff at the SHARE computer center had not received security awareness training and had only minimal training on security software used by the District.	ODC2/Security	Closed	This is an ongoing activity. OCTO provides proper training within budgetary constraints through CWD and professional education. Information Security Awareness is also identified as the part of the recently evolved OCTO ISP. OCTO hosted their 1 st Computer Security Awareness campaign on National Computer Security Awareness Day 11/30/01.
3.17 OCTO system programmers at the SHARE computer center had not received technical training on important types of system software, such as the tape management system.	ODC2	Closed	This is an ongoing activity. OCTO recognizes that technology and systems software is constantly evolving. OCTO provides proper training within budgetary constraints through CWD and professional education. Not all system programmers require training in all products.
3.18 None of District organizations visited were adequately promoting security awareness to ensure risks and responsibilities were understood.	Security	On-going	Regular awareness training will be scheduled and provided. Scheduled to begin November 30, 2001. Security awareness and training did begin on November 30 2001 and is ongoing.
3.19 Users were unaware of or insensitive to the need for important information system controls, such as a secure password.	Security	Closed	Should be promoted and will be implemented in conjunction with the previous item. (See Attachment 4, "Information Security Policy", for OCTO policy.)
3.20 None of the District organizations visited had established such a program, which would allow the District to identify and correct the types of weaknesses discussed in the report.	Security	Closed	This is still a problem. No central focal point established for correcting control weaknesses identified in this report. A District of Columbia Information Technology Security program has been established and is operational. This program under the Director is responsible for providing District-wide oversight, guidance, and accountability for IT security. This organization serves as the

GAO AUDIT ISSUES	RESPONSIBLE ORGANIZATION	STATUS	RESPONSE
	RACC	In-Progress	focal point for IT security within the DC government. See response from 3.6