GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

AUDIT OF CONTROLS OVER ACCESS TO THE SYSTEM OF ACCOUNTING AND REPORTING (SOAR)

CHARLES C. MADDOX, ESQ.
INSPECTOR GENERAL

OIG No. 00-02-05FL

September 28, 2001

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

September 28, 2001

Natwar M. Gandhi, Chief Financial Officer
Office of the Chief Financial Officer
441 Fourth Street, N.W., Room 1150 North
Washington, D.C. 20001

Dear Dr. Gandhi:

Enclosed is our final report (OIG No. 00-02-05FL) summarizing the results of our audit of controls over access to the System of Accounting and Reporting (SOAR). The audit evaluated access security controls over SOAR at the District agency level.

Specifically, our audit revealed that the SOAR Program Management Office (PMO) needed to:

- develop and implement formal policies and procedures to provide adequate training for agency security officers and
- develop and implement policies and procedures to provide for the decentralization of security administrator duties.

Factors causing these conditions include: insufficient training for agency security officers, less than optimal security administration procedures, and an ineffective method for monitoring users. Accordingly, this report contains recommendations that, collectively, represent actions considered necessary to correct the noted conditions.

The Office of the Chief Financial Officer (OCFO) comments (Exhibit A) to the draft of this report are generally responsive to the intent of the recommendations. However, Recommendation 2 remains unresolved. Therefore, OCFO should reconsider its position on Recommendation 2 to ensure that SHARE is notified by the agencies in a timely manner of deletions or modifications that would affect SOAR access resulting from employment status changes.

Generally, audit recommendations should be resolved within 6 months of the date of the final report. Accordingly, we will continue to work with OCFO to reach a final agreement on Recommendation 2. OCFO should reconsider Recommendation 2 and provide its response to our office by December 14, 2001.

We appreciate the cooperation and courtesies extended to our staff by OCFO and District agencies personnel during the audit. Further, we commend the OCFO and SOAR PMO management and staff for facilitating the audit process and recognizing the need to make systemic improvements.

If you have questions about this report please call me or William J. DiVello, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,

Charles C. Maddox, Esq.
Inspector General

Enclosure

See Distribution List Attached

DISTRIBUTION:

The Honorable Anthony A. Williams, Mayor, District of Columbia (1 copy)

Mr. Kelvin J. Robinson, Chief of Staff, Office of the Mayor (1 copy)

Mr. John A. Koskinen, Deputy Mayor and City Administrator (1 copy)

Ms. Germonique Jones, Staff, Mayor’s Press Office (1 copy)

Mr. Tony Bullock, Interim Director, Office of Communications (1 copy)

The Honorable Alice M. Rivlin, Chairman, DCFRA (1 copy)

Mr. Francis Smith, Executive Director, DCFRA (1 copy)

Mr. Johnnie Hemphill, Chief of Staff, DCFRA (5 copies)

The Honorable Linda W. Cropp, Chairman, Council of the District of Columbia (1 copy)

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 (1 copy)

Dr. Natwar M. Gandhi, Chief Financial Officer (4 copies)

Ms. Deborah K. Nichols, D.C. Auditor (1 copy)

Mr. Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO (1 copy)

Ms. Jeanette M. Franzel, Acting Director, Financial Management and Assurance, GAO (1 copy)

The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives (1 copy)

Mr. Jon Bouker, Office of the Honorable Eleanor Holmes Norton (1 copy)

The Honorable Joe Knollenberg, Chairman, House Subcommittee on D.C. Appropriations (1 copy)

Mr. Jeff Onizuk, Legislative Director, House Subcommittee on D.C. Appropriations (1 copy)

Mr. Migo Miconi, Staff Director, House Subcommittee on D.C. Appropriations (1 copy)

The Honorable Chaka Fattah, House Committee on D. C. Appropriations (1 copy)

Mr. Tom Forhan, Minority Staff Director, Office of the Honorable Chaka Fattah (1 copy)

The Honorable Connie Morella, Chairman, House Subcommittee on D.C. Government Reform (1 copy)

Mr. Russell Smith, Staff Director, House Subcommittee on D.C. Government Reform (1 copy)

Mr. Mason Alinger, Professional Staff Member, Senate Subcommittee on D.C. Government Oversight (1 copy)

The Honorable Richard Durbin, Chairman, Senate Subcommittee on D.C. Government Oversight (1 copy)

Ms. Marianne Upton, Staff Director, Senate Subcommittee on D.C. Government Oversight (1 copy)

The Honorable Mary Landrieu, Chairman, Senate Subcommittee on D.C. Appropriations (1 copy)

Ms. Kate Eltrich, Staff Director, Senate Subcommittee on D.C. Appropriations (1 copy)

Mr. Stan Skocki, Legislative Assistant, Senate Subcommittee on D.C. Appropriations (1 copy)

Mr. Charles Kieffer, Clerk, Senate Subcommittee on D.C. Appropriations (1 copy)

TABLE OF CONTENTS

EXECUTIVE DIGEST.. 1

OVERVIEW 1

CONCLUSIONS 1

CORRECTIVE ACTIONS 1

INTRODUCTION... 2

BACKGROUND 2

OBJECTIVE.. 2

SCOPE AND METHODOLOGY.. 2

FINDING AND RECOMMENDATIONS.................................. 4

SOAR SECURITY ACCOUNT MANAGEMENT 4

EXHIBIT

A. AGENCY RESPONSE TO DRAFT REPORT, FINDING, AND RECOMMENDATIONS

EXECUTIVE DIGEST

OVERVIEW

This report summarizes the Office of the Inspector General's (OIG) audit of security controls over the System of Accounting and Reporting (SOAR). SOAR is an integrated financial management system which provides information on budget, accounting, and assets. The District also uses SOAR to manage certain District-wide purchasing and financial reporting activities. The OIG performed this audit to determine whether adequate controls over SOAR access existed throughout District agencies.

CONCLUSIONS

Security administration over user access to the SOAR needed improvement. Specifically, neither the District agencies nor the SHARE computer center maintained sufficient supporting documentation of a user's initial access authorization, user access modifications, or user deletions from the system. These conditions existed because of less than optimal security administration procedures, insufficient training for agency security officers, and an ineffective method for monitoring system users. As a result, information in SOAR was at risk of unauthorized use, disclosure, revision, and loss.

CORRECTIVE ACTIONS

We addressed recommendations to the Director of the SOAR Program Management Office (PMO), that represent actions considered necessary to address the concerns described above. The recommendations, in part, center on:

- developing formal policies and procedures to provide adequate training for agency security officers and

- developing and implementing policies and procedures to provide for the decentralization of security administrator duties.

On August 23, 2001, the OCFO provided a written response to our draft report. The OCFO's responses were generally adequate to correct the conditions noted. However, Recommendation 2 remains unresolved. In order to resolve Recommendation 2, OCFO should reconsider its position on decentralized security administration to ensure that SHARE is notified by the agencies in a responsive manner of deletions and modifications resulting from employment status changes. The complete response is included at Exhibit A. Additionally, the OCFO comments are incorporated in the report where appropriate.

INTRODUCTION

BACKGROUND

In September 1997, the District awarded a contract to acquire a new financial accounting system to replace the District's aging Financial Management System (FMS). The District implemented SOAR on October 1, 1998, as the District's system of record.

The Office of the Chief Financial Officer (OCFO), Office of the Chief Information Officer (OCIO), and the SOAR Project Management Office (PMO) are responsible for providing administration and guidelines for SOAR access, usage, and training. In October 2000, the OCFO/OCIO transferred responsibility for managing the SHARE Computer Center, which is the location of the SOAR application, to the Office of the Chief Technology Officer (OCTO). Each District agency is responsible for appointing agency security officers, who coordinate with the SHARE Computer Center staff to facilitate granting user access.

OBJECTIVE

The objective of our review was to determine whether adequate access security controls over SOAR had been established throughout District agencies. However, after we started our audit, the General Accounting Office (GAO) started an audit of the Highway Trust Fund (GAO-01-489, dated April 2001), which included an evaluation and test of the overall effectiveness of the information system general controls over SOAR, which process the fund's financial data. The GAO audit objectives duplicated our original objectives but concentrated on the SHARE computer center level and not the District agency level. To minimize any duplication of efforts, we modified our objectives and focused our review on access security controls over SOAR at the District agency level.

SCOPE AND METHODOLOGY

The scope of our review generally covered the period of November 2000 to March 2001. Our audit was limited to 12 agencies that were randomly selected from 64 agencies.[1] These 12 agencies had 3,346 user logon IDs with access to SOAR.

We used the following methodology in gathering data and conducting tests to ensure completion of our stated objectives:

- visited selected agencies to evaluate the effectiveness of SOAR access controls;

[1] These agencies were selected from an agency listing published by the Office of Financial Operations and Systems.

INTRODUCTION

- conducted interviews with responsible management personnel and agency security officers;

- identified and reviewed security policies and procedures relating to access security;

- identified and documented access levels of security; and

- coordinated, as necessary, our work with that of the General Accounting Office.

Our audit was conducted in accordance with generally accepted government auditing standards.

FINDING AND RECOMMENDATIONS

FINDING: SOAR SECURITY ACCOUNT MANAGEMENT

SYNOPSIS

Security administration over user access to the System of Accounting and Reporting (SOAR) needed improvement. Specifically, neither the District agencies nor the SHARE computer center maintained adequate supporting documentation of a user's initial access authorizations, access modifications, or user deletions from the system. These conditions existed because of less than optimal security administration procedures, insufficient training for agency security officers, and an ineffective method for monitoring system users. As a result, information in SOAR is at risk of unauthorized use, disclosure, revision, and loss.

DISCUSSION

Our review revealed that agencies did not maintain supporting documentation of users' initial access authorizations or deletions from the system. This resulted from: 1) non-optimal security administration procedures used to assign and monitor user IDs with SOAR access privileges; 2) ineffective methods for monitoring user access request activity; and 3) insufficient training for agency security officers.

The SOAR Security Access Policy and Procedures provides instructions on the process to follow and the necessary forms required in order for employees to gain access to SOAR. Specifically, these procedures require that supervisors complete and submit specific documents to SHARE and the SOAR Program Office to obtain a user ID, LOGON ID, and requests for modification or terminations of user ID's for all employees. Additionally, these procedures require supervisors and agency security officers to communicate all actions for SOAR access to the centralized security administrators located at the SHARE computer center.

Our audit determined that these policies and procedures did not specifically provide requirements for agency security officers to follow-up on access request actions or to conduct a periodic review of user access requirements. As a result, the procedures governing SOAR system security matters did not provide for an optimal level of security administration.

Currently, two SHARE computer center employees are responsible for the overall Access Control Facility 2 (ACF-2)[2] security administration and monitoring of all users.

[2] ACF-2 is a data protection system that provides controlled sharing of data.

FINDING AND RECOMMENDATIONS

This form of centralized security administration is not efficient for administering the approximate 5,299[3] user logon IDs maintained in the ACF-2 security application's user database. The current procedure requires the SHARE computer center security personnel's involvement in each action that adds, deletes, or modifies user logon IDs, which results in a lengthy turn-around time for user access processing. We believe that the decentralization of security at the District agency level would improve the security administration for agency users' access requests.

We used a listing of all user logon IDs and related application access privileges listed in the SHARE security application's database. From that listing, we randomly selected 12 agencies to determine if these agencies maintained adequate supporting documentation for users having access to SOAR.

We found that the 12 agencies did not have access request forms or other supporting documentation for 966 of 3,346 user logon IDs with SOAR access privileges. Below is a table summarizing the results of our review.

Agency	Number of user logon IDs	Number of logon IDs With Access Request Forms and/or Supporting Documentation	Number of logon IDs Without Access Request Forms and/or Supporting Documentation
Mission Support/Office of the Chief Financial Officer[4]	702	180	522
Metropolitan Police Department	61	37	24
D.C. Fire & Emergency Medical Services	447	432	15
Department of Corrections	80	17	63
D.C. Public Schools	1136	1071	65
Department of Human Services	112	28	84
D.C. Office of Personnel	108	48	60
University of the District of Columbia	177	140	37
Department of Public Works	137	74	63
DHS/Commission on Mental Health	386	353	33
Totals	**3346**	**2380**	**966**

[3] Total number of user logon IDs, as reported by GAO, in the SHARE computer center's ACF-2 security software database.

[4] The Office of the Chief Financial Officer administers user access for the Offices of Tax and Revenue, Chief Information Officer, Grants Management and Development, Budget and Planning, Financial Operations and Systems, Executive Director, and Finance and Treasury.

FINDING AND RECOMMENDATIONS

We determined that the agency security officers who were responsible for the administration of user access privileges could not explain the differences or provide documentation that supported the differences between the lists. All users on the system should have an access request document. Additionally, based on limited testing, we found 6 SOAR users with active logon IDs and passwords who remained on the system from 11 to 335 days after a change in employment and 7 SOAR users had multiple passwords.

Furthermore, the SOAR PMO had not established a SOAR security training program for its agency security officers. This condition makes it difficult to establish effective system security monitoring and hinders the ability of security officers to follow up on potential security violations. Accordingly, sufficient training and knowledge of system security control concepts should be provided to all agency security officers.

In May of 2001, the SOAR PMO issued revised policies and procedures to address the deficiencies identified above. Specifically, the update of the SOAR Security Access Policy and Procedures now mandates that each District agency keep copies of supporting documentation, to include access request/modification/termination forms for all requested user access activity. This will assist in further strengthening controls to ensure that access capabilities initially granted are still required. Additionally, the policies provide for periodic revalidation of user logon IDs to determine if a user’s access privileges are still needed.

RECOMMENDATIONS

We recommend that the Director of the SOAR PMO:

1. Develop and implement formal policies and procedures to ensure adequate training for agency security officers. This would allow agency security officers to effectively monitor SOAR and to trace and follow up on potential security violations.

2. Decentralize security documentation and monitoring currently conducted centrally at the SHARE computer center level to the District agency level.

OCFO RESPONSES

Recommendation 1. The OCFO concurs with the recommendation. In April 2001, the policies and procedures for SOAR users were completed, and formed the basis of the training manual on the subject. Training for the agency security officers began shortly thereafter, but due to limitations was suspended to give priority to other needed training programs. Although classroom training will resume in late August 2001, the

FINDING AND RECOMMENDATIONS

agency security officer training has been conducted at a few agencies where it was convenient to do so.

Recommendation 2. The OCFO did not concur with our recommendation. The OCFO responded that the SOAR PMO has no control over the issuance of SHARE logon IDs, and that the responsibility for that function rests solely with the OCTO. The OCFO further responded that SOAR is but one application that runs on the SHARE data center network and stated that our report did not address the effects that decentralized access would have on the other applications and how controls currently in place would be achieved.

OIG COMMENTS

The action completed by the SOAR PMO in response to Recommendation 1 should resolve the conditions noted. It is encouraging that the SOAR PMO initiated corrective action before our audit was completed.

The OCFO comments for Recommendation 2 are noted. The OIG report acknowledged that in October 2000, responsibility for providing administration and guidelines over SOAR access, usage, and training was transferred to the Office of the Chief Technology Officer (OCTO). However, we addressed the recommendation to the SOAR PMO because it is the SOAR PMO who is also responsible for administering the District's System of Accounting and Reporting (SOAR) security. Although OCTO has control over the issuance of SHARE logon IDs, we believe that the current procedure - which requires SHARE security personnel's involvement in each action that adds, deletes, modifies user logon IDs and requires three business days to process - could be more effective through the use of decentralized security administration. For example, we noted SOAR users with active logon ID privileges who had remained on the system for an extended period of time after a change in employment status and users with multiple passwords.

With decentralized security administration, appointed agency security officers could be given the ACF-2 Account attribute, which would allow appointed agency security officers to establish, maintain, and delete user logon IDs within their scope of authority. In addition to reducing the workload of SHARE security personnel, it also establishes a separation of functions between the agencies and SHARE. Since it is incumbent upon the agency security officer to provide SHARE with documentation requesting access and modification to user logon IDs and passwords, there should be a process to ensure that SHARE is notified by the agency or the Personnel Department in a timely manner of deletions or modifications resulting from employment status changes.

FINDING AND RECOMMENDATIONS

The OIG believes that the agency security officer's proximity to the users and understanding of the employment statuses and changes within their respective organizations would allow them to respond quicker to access requests and modifications within their organization. Furthermore, proper training would allow agency level personnel to take full advantage of all the security control capabilities within the ACF-2 access control security software. If deemed necessary the OCFO should coordinate this corrective action with OCTO.

Exhibit A

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Chief Financial Officer

Natwar M. Gandhi
Chief Financial Officer

August 23, 2001

Mr. Charles C. Maddox, Esq.
Inspector General
Office of the Inspector General
717 14th Street, N.W.
Washington, DC 20005

Dear Mr. Maddox:

This is in response to your August 7, 2001 letter regarding the draft report (OIG No. 00-02-05-FL), which summarized the results of your audit of controls over the access to the System of Accounting and Reporting (SOAR).

The draft report acknowledges that the responsibility for SHARE (which issues Log-On Ids) was transferred to the Office of the Chief Technology Officer (OCTO). However, in the recommendations to the Director of the SOAR PMO, that fact was not taken into consideration.

The OIG recommended that the Director of the SOAR PMO to develop and implement formal policies and procedures to ensure adequate training for agency security officers. This would allow agency security officers to effectively monitor the SOAR system and to trace and follow up on potential security violations.

The OCFO concurs with this recommendation. Prior to the Office of the Inspector General (OIG) performing its audit, the SOAR PMO Office had recognized the need to (1) document policies and procedures for SOAR users, and (2) train Agency Security Administrators (ASAs). In April 2001, the Policy and Procedures document (Exhibit 1) was completed, and formed the basis of the training manual (Exhibit 2) on the subject. This information was provided to the OIG auditors for their information and record. Training for the ASAs began shortly thereafter, but due to limitations of out-training resources, it was temporarily suspended to give priority to other needed training programs. Although classroom training will resume in late August 2001, our security officer has conducted the ASA training at a few agencies where it was convenient to do so.

The OIG recommended that the Director of the SOAR PMO decentralize security documentation and monitoring currently conducted centrally at the SHARE computer center level to the District agency levelL

The OCFO does not concur with this recommendation. The Director of the SOAR PMO has no control over the issuance of SHARE Log-On Ids. Responsibility for that function rests solely with the OCTO. SOAR is but one application that runs on the SHARE data center network. We also noted that your report does not address the effects that decentralized access would have on the other applications and how the controls currently in place would be achieved.

With regard to decentralized SOAR access, the finding of this draft report supports the opinion of this office that it is premature to consider decentralizing the security access to agencies at this time. The Office of Internal Audit and Internal Security (IAIS) will be requested to perform compliance audits of these polices and procedures and to make recommendations as appropriate.

If you have any questions, please contact me at (202) 727-2476, or your staff may contact [redacted] at [redacted], or [redacted] at [redacted].

Sincerely,

Natwar M. Gandhi
Chief Financial Officer

Enclosures