AUDIT REPORT

CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Audit Report on User Access Controls at the Department of Finance

7A03-133

June 26, 2003

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341
- - - - - - - - - - - - - -
WILLIAM C. THOMPSON, JR.
COMPTROLLER

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the Comptroller's responsibilities contained in Chapter 5, § 93, of the New York City Charter, my office has performed an audit of the User Access Controls at the Department of Finance. The results of our audit, which are presented in this report, have been discussed with officials from the Department of Finance, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that the City has adequate controls in place to protect its records from unauthorized access.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please contact my audit bureau at 212-669-3747 or e-mail us at audit@Comptroller.nyc.gov.

Very truly yours,

William C. Thompson Jr

William C. Thompson, Jr.

WCT/GR

Report: **7A03-133**
Filed: **June 26, 2003**

Table of Contents

AUDIT REPORT IN BRIEF 1

INTRODUCTION 2

- Background 2
- Objective 3
- Scope and Methodology 3
- Discussion of Audit Results 4

FINDINGS AND RECOMMENDATIONS 5

- Information Protection Policies and Procedures Not Complete 6
- Lack of Procedures to Identify and Eliminate IDs of Inactive Users and Users Who Leave City Service 6
- Reviews of User Privileges Not Performed in a Timely Manner 6
- Credit Card Information Not Encrypted 7
- Lack of Virus Response Plan 7
- Network Access Weaknesses 7
- Recommendations 7

ADDENDUM – Department Response

Bureau of Financial Audit
EDP Audit Division

Audit Report on User Access Controls at the Department of Finance

7A03-133

AUDIT REPORT IN BRIEF

We performed an audit of the user access controls at the Department of Finance (Department). The Department of Information Technology and Telecommunications (DoITT) manages the Department's system software and hardware and provides software-based controls that help the Department control access to computer systems and to specific data or functions within the systems. The mainframe security program used by DoITT to protect resources such as databases and application programs is Resource Access Control Facility (RACF). For the network environment, such as the Internet and the wide area network, DoITT maintains a secure portal that allows the Department to send and receive information from the Internet and other communications links, such as Citynet. The Department is responsible for assigning RACF user profiles and application controls to specific applications in the both the mainframe and network environments.

Audit Findings and Conclusions

The Department has adequate controls to protect both its mainframe and network environments. The Department and DoITT have a number of procedures to control data, files, and applications. However, there were several security matters that should be addressed. Specifically, for the mainframe environment, the Department's information protection policies and procedures are not consolidated in one formal document, and some of the Department's policies were last updated as far back as 1989. Further, there are no formal procedures in place for identifying and eliminating user IDs for inactive users and individuals who leave City service. Also, the Department does not perform timely reviews and updates of employee system privileges.

At the network level, the Department has no formal information protection policies and procedures for the network environment, and the system does not encrypt credit card information received from the public. Moreover, the Department has no agency virus response plan, and network applications do not automatically suspend inactive user accounts.

Audit Recommendations

To address these issues, we recommend that the Department:

- Update its information protection policies and procedures, in accordance with Comptroller's Directive 18. The Department should ensure that these policies and procedures include the network environment.

- Develop procedures for identifying and eliminating user IDs for inactive users and individuals who leave City service. Immediately review the current list of users and make the appropriate adjustments

- Perform timely reviews and updates of employee system privileges.

- Ensure that all credit card information on the system is encrypted.

- Immediately develop and implement a formal virus response plan, in accordance with Comptroller's Directive 18.

- Modify the network security software to automatically suspend user accounts if they are not used for a specified period of time.

INTRODUCTION

Background

The Department of Finance (Department) administers and enforces tax laws and collects taxes, judgments, and other charges levied by a number of City agencies and courts. The Department: educates the public about its rights and responsibilities with regard to taxes; processes parking summons; provides motorists with a forum to contest summonses through an adjudication hearing; and collects court-ordered private and public sector debt.

The Department of Information Technology and Telecommunications (DoITT) manages the Department's system software and hardware. Further, DoITT administers access controls to information stored in the Department's 16 mainframe applications as well as to two kiosk-based applications in the network environment that supports Department activities.

DoITT provides software-based controls containing a variety of programmed features that help the Department control access to computer systems and to specific data or functions within the systems. The mainframe security program used by DoITT to protect resources—such as databases, application programs, and the mainframe operating system—is Resource Access Control Facility (RACF). For the network environment (Internet access, the local area network, and the wide area network), DoITT maintains a secure portal that allows the Department to send and receive information from the Internet and other communications links, such as Citynet, the Citywide area network. Once the information passes through DoITT, the Department has its own firewalls and intrusion detection system.

The Department is responsible for assigning RACF user profiles and application controls (the automated controls programmed into each specific application) to specific applications in both the mainframe and network environments.

Objective

This audit determined whether adequate user access controls are in place to protect information in the Department's computerized environment from unauthorized access.

Scope and Methodology

Our fieldwork was conducted from January 2003 through April 2003. To achieve our objectives, we:

- Interviewed Department officials and security personnel from the Information Systems Service group and IBM representatives who developed the Department's network security structure;
- Reviewed background material;
- Reviewed and analyzed security policies and procedures;
- Reviewed and analyzed a RACF user list for the Department mainframe environment; and
- Randomly selected 168 RACF users from the 657 users in the Department that could not be matched to the New York City Payroll Management System (PMS) to determine whether accounts were appropriately deleted from the system when employees left City service.

To meet our audit objectives, we used Comptroller's Directive 18, the National Institute of Standards and Technology (NIST) *Generally Accepted Principles and Practices for Securing Information Technology Systems* § 3.5.2, and information security guidelines developed by the New York City Department of Investigation, as a criteria for this audit. In addition, we reviewed relevant sections of the New York City Charter.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the audit responsibilities of the City Comptroller, as set forth in Chapter 5, § 93, of the New York City Charter.

Discussion of Audit Results

The matters covered in this report were discussed with Department officials during and at the conclusion of this audit. A preliminary draft was sent to Department officials and was discussed at an exit conference held on June 6, 2003. On June 11, 2003, we submitted a draft report to Department officials with a request for comments. We received a written response from the Department on June 20, 2003. The Department stated that it will implement all six recommendations. The full text of the Department's comments is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

The Department has adequate controls to protect both its mainframe and network environments. The Department and DoITT have a number of procedures to control data, files, and applications.

At the mainframe level, the Department and DoITT have:

- Security policies and procedures (although these policies and procedures should be updated);
- A requirement that RACF users change passwords every 30 days;
- User passwords that are unique;
- Passwords that are automatically disabled after 30 days of inactivity;
- Special administrative access that is restricted to a minimal number of administrators; and
- Automatic deactivation of users after three failed log-on attempts.

However, there were several security matters that should be addressed. Specifically, for the mainframe environment, the Department's information protection policies and procedures are not consolidated in one formal document, and some of the Department's policies were last updated as far back as 1989. Further, there are no formal procedures in place for identifying and eliminating user IDs for inactive users and individuals who leave City service. Also, the Department does not perform timely reviews and updates of employee system privileges.

At the network level, the Department and DoITT have:

- Cisco firewalls and two intrusion detection systems to prevent the unauthorized entry or attacks from either the Internet web server or the Intranet web server;
- Virus detection software that is updated weekly; and
- Automatic deactivation of users after three failed log-on attempts.

The Department has no formal information protection policies and procedures for the network environment, and the system does not encrypt credit card information received from the public. Moreover, the Department has no formal virus response plan, and network applications do not automatically suspend inactive user accounts.

These issues are addressed in the following sections.

Information Protection Policies and Procedures Not Complete

The Department's information protection policies are outdated, incomplete, and have not been assembled in one comprehensive document. The Department's procedures, some of which were last updated in 1989, do not address: the identification and investigation of invalid log-on attempts, the use of intrusion detection software, and the elimination of accounts of employees who have left City service. Further, the information protection policies and procedures do not address the agency's network environment. Comptroller's Directive 18, § 5.0, states:

> "The information protection plan establishes both broad general policies and the day to day internal controls, procedures and practices agencies must implement to safeguard the information processing environment against the risks and vulnerabilities identified in the assessment phase. The most effective plans are comprehensive, covering all aspects of the information processing environment and are in written form."

In addition, Comptroller's Directive 18, § 9.6, states that "to be effective, information protection policies and procedures . . . should be reviewed and updated periodically, but no less than biennially."

Lack of Procedures to Identify and Eliminate IDs of Inactive Users and Users Who Leave City Service.

The Department has no formal procedures to identify and eliminate user IDs of inactive users and individuals who leave City service. We found that 54 of our 168 sampled users were not listed on PMS as employees of the Department. In addition, the names on the RACF user list for the remaining 114 sampled users did not initially match to PMS because of misspellings; however, further testing enabled us to link these user IDs to individuals on PMS. Comptroller's Directive 18, § 8.1.2, states, "Active password management includes . . . (3) Deactivation of inactive user accounts and accounts for employees whose services have terminated."

Reviews of User Privileges Not Performed in a Timely Manner

The Department does not perform timely reviews of employees' system privileges. The National Institute of Standards and Technology (NIST), *Generally Accepted Principles and Practices for Securing Information Technology Systems* § 3.5.2, states, "Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access."

Agency managers receive an annual survey showing the level of RACF authority assigned to their staff. The managers are given three months to review and advise the system security administrator of any necessary changes to the level of each user's authority. Consequently, it could take the Department 15 months to modify or delete system privileges of employees who change job functions or leave City service.

Credit Card Information Not Encrypted

The Department does not encrypt credit card information received from the public at its six business centers and 12 kiosks. Comptroller's Directive 18, §9.1.3, states, "For all networks, especially those connected to the Internet, managers should . . . (6) Employ data encryption and one-time passwords when data communications are particularly sensitive, such as in the transmission of credit card information."

Lack of Virus Response Plan

The Department does not have a formal virus response plan, as required by Comptroller's Directive 18, which states, "Protection against software viruses requires a combination of software based and procedural access controls . . . [and a] (5) Response Plan-A formal response plan that can quickly be put into action when a virus is detected."

Network Access Weaknesses

The Department's network security software does not automatically suspend a user account if it is not used for a specified period of time. Comptroller's Directive 18, § 8.1.2, states, "Active password management includes: (1) Insuring that users are forced to change passwords periodically; [and] . . .(3) Deactivation of inactive user accounts and accounts for employees whose services have terminated." In addition, the network applications permit users to have multiple IDs and passwords, which increases the risk of unauthorized access to the system.

Recommendations

The Department should:

1. Update its information protection policies and procedures, in accordance with Comptroller's Directive 18. The Department should ensure that these policies and procedures include the network environment.

Department Response: "Finance agrees with the recommendation to update its polices and procedures in accordance with Directive 18 and Finance will ensure that the network environment is included in the update process. ISS [Information

Systems Services] will work with senior management to develop the policies. We expect the improvements to be in place by end of calendar year 2003."

2. Develop procedures for identifying and eliminating user IDs for inactive users and individuals who leave City service. Immediately review the current list of users and make the appropriate adjustments.

<u>Department Response</u>: "Finance agrees with the recommendation to develop formal procedures for identifying and eliminating user IDs for inactive users and for individuals who leave City service. Documentation of this internal process will be developed by the end of calendar year 2003. During Fiscal Year 2004, Finance's Internal Audit Unit plans to review the user ID update procedures."

3. Perform timely reviews and updates of employee system privileges.

<u>Department Response</u>: "Finance agrees with this recommendation. Accordingly, Finance will reduce the amount of time that managers are allowed between when the review is started to the time the changes must be returned to ISS. In the future, managers at Finance will have two weeks to review the list. Managers at agencies other than Finance will have three weeks (the extra week to allow for the delivery time of the documents). Additionally, to maintain security level consistency, no changes to security levels during the period of review will be accepted. This new procedure will begin immediately. During Fiscal Year 2004, Finance's Internal Audit Unit is scheduled to review employee system privileges procedures."

4. Ensure that all credit card information on the system is encrypted.

<u>Department Response</u>: "Finance agrees that the transfer of all credit card information between cashiers and Kiosk workstations to Finance's internal servers should be encrypted. We will start a project to implement encryption in 2003."

5. Immediately develop and implement a formal virus response plan, in accordance with Directive 18.

<u>Department Response</u>: "Finance agrees with the recommendation to develop a formal virus response plan. A formal plan will be developed to comply with Comptroller's Directive 18 and DOI [Department of Investigation] Directives published at the DOI/CISAFE [Citywide Information Security Architecture Formulation and Enforcement Unit] web site by the end of calendar year 2003."

6. Modify the network security software to automatically suspend user accounts if they are not used for a specified period of time."

<u>Department Response</u>: "Finance agrees with the recommendation that network security should suspend inactive user accounts. However, NT network security does not have an automatic process to suspend inactive accounts. ISS will investigate implementation of a scheduled batch job to identify inactive accounts for manual suspension or the procurement of third party software to do so. ISS expects to begin this project no later than fourth quarter calendar year 2003."

FINANCE
NEW • YORK
THE CITY OF NEW YORK
DEPARTMENT OF FINANCE

BY FAX AND HAND-DELIVERY

June 20, 2003

Mr. Greg Brooks
Deputy Comptroller
Office of the Comptroller
1 Centre Street
New York, NY 10007

Re: Audit # 7A03-133
Audit Report on User Access
Controls at the Department of Finance

Dear Mr. Brooks,

Thank you for the opportunity to review and comment on the above referenced draft audit. The audit was helpful to our Information Systems Services Division (ISS) because it highlights areas where we can improve. The report suggests that Finance implement six recommendations. Below are the recommendations made in the draft report, and Finance's comments on the recommendations:

The Department of Finance should:

1. Update its information protection policies and procedures, in accordance with Comptroller's Directive 18. The Department should ensure that these policies and procedures include the network environment.

   Finance agrees with the recommendation to update its polices and procedures in accordance with Directive 18 and Finance will ensure that the network environment is included in the update process. ISS will work with senior management to develop the policies. We expect the improvements to be in place by end of calendar year 2003.

2. Develop procedures for identifying and eliminating user IDs for inactive users and individuals who leave City service. Immediately review the current list of users and make appropriate adjustments.

   Finance agrees with the recommendation to develop formal procedures for identifying and eliminating user IDs for inactive users and for individuals who leave City service. Documentation of this internal process will be developed by the end of calendar year 2003. During Fiscal Year 2004, Finance's Internal Audit Unit plans to review the user ID update procedures.

3. Perform timely reviews and updates of employee system privileges.

   Finance agrees with this recommendation. Accordingly, Finance will reduce the amount of time that managers are allowed between when the review is started to the time the changes must be returned to ISS. In the future, managers at Finance will have two weeks to review the list. Managers at agencies other than Finance will have three weeks (the extra week is to allow for the delivery time of the documents). Additionally, to maintain security level consistency, no changes to security levels during the period of review will be accepted. This new procedure will begin immediately. During Fiscal Year 2004, Finance's Internal Audit Unit is scheduled to review employee system privileges procedures.

4. Ensure that all credit card information on the system is encrypted.

   Finance agrees that the transfer of all credit card information between cashiers and Kiosk workstations to Finance's internal servers should be encrypted. We will start a project to implement encryption in 2003.

5. Immediately develop and implement a formal virus response plan, in accordance with Directive 18.

   Finance agrees with the recommendation to develop a formal virus response plan. A formal plan will be developed to comply with Comptroller's Directive 18 and DOI Directives published at the DOI/CISAFE web site by the end of calendar year 2003.

6. Modify the network security software to automatically suspend user accounts if they are not used for a specified period of time.

   Finance agrees with the recommendation that network security should suspend inactive user accounts. However, NT network security does not have an automatic process to suspend inactive accounts. ISS will investigate implementation of a scheduled batch job to identify inactive accounts for manual suspension or the procurement of third party software to do so. ISS expects to begin this project no later than fourth quarter calendar year 2003.

Thank you again for the opportunity to review and comment on the draft report.

If you have any questions concerning this response, please feel free to call me at (212) 669-4878.

Sincerely,

Carla Van de Walle

Carla Van de Walle

cc: Martha E. Stark, Commissioner, Department of Finance
George Davis, III, Deputy Director, Mayor's Office of Operations
George Mark, Assistant Commissioner, Department of Finance,
Information Systems Services