The City of New York
Office of the Comptroller
Bureau of Financial Audit
EDP Audit Division

WILLIAM C. THOMPSON, JR.
Comptroller

Follow-up Audit of the Department of Correction Local Area Network

7F02-162

June 24, 2002

The City of New York
Office of the Comptroller
Bureau of Financial Audit
EDP Audit Division

Follow-up Audit of the Department of Correction Local Area Network

7F02-162

SUMMARY OF FINDINGS AND CONCLUSIONS

This is a follow-up audit to determine whether the Department of Correction (DOC) implemented the seven recommendations made in a previous audit, *Audit of the Department of Correction Local Area Network* (Audit No.7A98-140, issued June 15, 1998). The earlier audit focused on DOC's Local Area Network (DOCNET) and evaluated the adequacy of DOC's policies and procedures regarding its hardware and software inventory controls, capital project funds recording system, anti-virus measures, and access security controls. The prior audit reported deficiencies in DOC's inventory control system, recording procedures of the Fixed Asset Inventory Report, virus protection, and access security control system. In our current audit, we discuss the recommendations we made in the previous report, as well as the implementation status of those recommendations. An additional objective was to evaluate DOC compliance with Department of Investigation (DOI) system security standards, which require agencies that plan to provide agency-wide Internet access to submit an Internet Security Architecture Plan. We also discuss new findings and recommendations based on our current review.

Of the seven recommendations contained in the previous report, four have been implemented and three have not been implemented. The evaluation of DOC's compliance with DOI security system standards disclosed that DOC submitted a Security Architecture Proposal to DOI and received approval from DOI. DOC is in the process of developing related forms and documentation. The details of the earlier recommendations and their current implementation status follow. We recommended that:

1. "DOC's Manager of PC Support and its Manager of LAN Support purchase an automated inventory control system. The information to be contained in this system should include, but not be limited to, equipment type, manufacturer, model number, serial number, location, asset tag number, and purchase order information." **IMPLEMENTED**

2. "DOC's Executive Director of MIS [DOC's Management Information Systems group] produce written inventory control procedures for using the new inventory

control system to monitor the status of equipment from the time it is received from the vendor until the time it is salvaged." **IMPLEMENTED**

3. "DOC's Purchasing Manager follow the proper procedures to ensure that new equipment is added and maintained on the IFMS [Integrated Financial Management System] Fixed Assets System. He should also ensure that retired/obsolete equipment is removed from the IFMS Fixed Assets System." **NOT IMPLEMENTED**

4. "DOC's Manager of PC Support and its Manager of LAN Support purchase and install a software package that allows them to track the different software applications on the workstations that are connected to the network." **IMPLEMENTED**

5. "DOC's Manager of PC Support and its Manager of LAN Support use the information from the application tracking software, once it has been installed, to ensure that all software applications are properly licensed." **NOT IMPLEMENTED**

6. "DOC's Manager of PC Support and its Manager of LAN Support purchase and install anti-virus software that offers a combination of server and client protection. We informed the above managers of one anti-virus software package that detects viruses on MS DOS products that run on servers with the Open VMS operating system, such as DOCNET." **IMPLEMENTED**

7. "DOC's Data Center Manager and its Systems Programming Manager review all the accounts with special privileges, that they determine the number of accounts that can be removed, and that they remove these accounts." **NOT IMPLEMENTED**

We now recommend that DOC should:

1. Record new computer equipment on the Financial Management System (FMS)[1], and remove retired or obsolete equipment from FMS.

2. Review all accounts with special privileges to the Open VMS Operating System to determine the number of accounts that can be removed, and remove these accounts.

3. Create a written policy that prevents the illegal copying or pirating of its software and software documentation and that prevents the installation of illegal software on the network.

4. Review its software inventory and delete all illegal software.

[1] As of July 1, 1999, the Financial Management System replaced IFMS.

5. Review and update its inventory policies and procedures.

We conducted this follow-up audit 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 City Comptroller's audit responsibilities as set forth in Chapter 5, § 93, of the New York City Charter.

Agency Response

The matters covered in this report were discussed with officials from DOC during and at the conclusion of this audit. A preliminary draft report was sent to DOC officials and discussed at an exit conference held on May 29, 2002. On May 30, 2002 we submitted a draft report to DOC officials with a request for comments. We received a written response from DOC on June 13, 2002. DOC agreed to implement four of the five recommendations made in this report. With regard to the remaining recommendation, DOC's response indicated that it reviewed user accounts that had special privileges and that removal was not possible because "to remove any privileges from these accounts would render the systems non-functional." The full text of the DOC comments is included as an addendum to this report.

INTRODUCTION

Background

The Department of Correction (DOC) provides custody, control, and care of felons sentenced to one year of incarceration or less; detainees awaiting trial or sentence; newly sentenced felons awaiting transportation to State correctional facilities; alleged parole violators awaiting revocation hearings; and State prisoners awaiting court appearances in New York City. DOC maintains a safe and secure environment for staff, inmates, and the public by pursuing a policy of zero tolerance for gang-related and other criminal activity in its facilities. Through its self-contained emergency response capability, DOC is able to respond to full-scale citywide emergencies and disasters. DOC handles approximately 120,000 admissions each year, manages an average daily inmate population of approximately 15,000 individuals, and transports an average of approximately 1,500 individuals to court facilities each business day.

DOC's Management Information Systems group (MIS) maintains DOC's Local Area Network (LAN), known as DOCNET. DOCNET's servers are located in DOC's headquarters data center and connect approximately 1,500 workstations. The workstations are located throughout DOC's headquarters and its four other sites. MIS provides DOCNET support, maintains computer systems, controls access security, and manages computer inventory control systems.

Objectives, Scope, and Methodology

This follow-up audit was initiated to determine whether the seven recommendations contained in a previous audit, *Audit of the Department of Correction Local Area Network* (Audit No. 7A98-140, issued June 15, 1998), were implemented. An additional objective was to evaluate DOC's compliance with the Department of Investigation (DOI) system security standards, which require agencies that plan to provide agency-wide Internet access to submit an Internet Security Architecture Plan.

Audit fieldwork began in March 2002 and ended in May 2002. To meet our objectives, we:

- interviewed DOC officials;
- evaluated DOCNET access security controls;
- examined DOC's computer inventory control system;
- evaluated DOC's procedures for recording fixed assets;
- reviewed DOC's Internet connectivity plan; and

- tested DOC’s compliance with Comptroller’s Directive #18.

We used Comptroller’s Internal Control and Accountability Directive #18 and the DOI *Standards for Inventory Control and Management* as our audit criteria.

We conducted this audit 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 City Comptroller’s audit responsibilities as set forth in Chapter 5, § 93, of the New York City Charter.

Agency Response

The matters covered in this report were discussed with officials from DOC during and at the conclusion of this audit. A preliminary draft report was sent to DOC officials and discussed at an exit conference held on May 29, 2002. On May 30, 2002 we submitted a draft report to DOC officials with a request for comments. We received a written response from DOC on June 13, 2002. DOC agreed to implement four of the five recommendations made in this report. With regard to the remaining recommendation, DOC’s response indicated that it reviewed user accounts that had special privileges and that removal was not possible because “to remove any privileges from these accounts would render the systems non-functional.” The full text of the DOC comments is included as an addendum to this report.

OFFICE OF THE COMPTROLLER
NEW YORK CITY

DATE FILED: June 24, 2002

RESULTS OF THIS FOLLOW-UP AUDIT

PREVIOUS FINDING: "DOC maintains neither a manual nor an automated perpetual inventory system to provide an up-to-date count of its personal computers and printers at any given time."

Previous Recommendation #1: "We recommend that DOC's Manager of PC Support and its Manager of LAN Support purchase an automated inventory control system. The information to be contained in this system should include, but not be limited to, equipment type, manufacturer, model number, serial number, location, asset tag number, and purchase order information."

Previous Agency Response: "MIS will comply with this recommendation. MIS has purchased an integrated help desk and inventory package."

Current Status: IMPLEMENTED

DOC purchased TrackIt software to monitor information about its computer equipment inventory. This automated inventory control package contains the recommended information, such as equipment type, manufacturer, model number, serial number, location, and asset tag number of the computer equipment. Although the system does not include purchase-order information, it conforms to the DOI Inventory Control Standard. We therefore consider Recommendation #1 implemented.

Previous Recommendation #2: "We recommend that DOC's Executive Director of MIS produce written inventory control procedures for using the new inventory control system to monitor the status of equipment from the time it is received from the vendor until the time it is salvaged."

Previous Agency Response: "MIS will comply with this recommendation."

Current Status: IMPLEMENTED

DOC provided written procedures and policies dated April 30, 1997, for the inventory control system and for monitoring equipment. Accordingly, we consider Recommendation #2 implemented.

****

PREVIOUS FINDING: "New computer equipment is not recorded on the IFMS Fixed Assets accounting report."

Previous Recommendation #3: "We recommend that DOC's Purchasing Manager follow the proper procedures to ensure that new equipment is added and maintained on the IFMS

Fixed Assets System. He should also ensure that retired/obsolete equipment is removed from the IFMS Fixed Assets System."

__Previous Agency Response__: "MIS does follow the proper procedures with regard to the IFMS Fixed Assets System . . .. The equipment [used for DOCNET] consists of items, largely PCs and printers, all of which cost less than $15,000 each. Moreover the minimum useful life of a PC, is by no stretch of the imagination, five years. Therefore this equipment does not belong on the IFMS Fixed Assets System."

__Current Status__: NOT IMPLEMENTED

DOC purchased 119 personal computers, at a cost of $208,514, and 125 printers, at a cost of $98,942, during 2001. These items, which were purchased through the Capital Budget, were not listed in the FMS Fixed Asset Inventory Report. We also noted that equipment reported in the previous audit (purchased in 1984 and 1985) that is reportedly no longer in use is still listed on the Fixed Asset Inventory Report. Accordingly, we consider Recommendation #3 not implemented.

****

__PREVIOUS FINDING:__ "DOC has neither a manual nor an automated system to keep an up-to-date inventory of software installed on DOCNET workstations. Without such a system, it is difficult to ensure that all software applications on the network are properly licensed. In addition there is no way of knowing if individual users have installed other unlicensed software packages on their workstations."

__Previous Recommendation #4__: "To ensure that unlicensed software packages are not installed on DOCNET workstations, we recommend that DOC's Manager of PC Support and its Manager of LAN Support purchase and install a software package that allows them to track the different software applications on the workstations that are connected to the network."

__Previous Agency Response__: "MIS has already purchased the necessary software for 'tracking' the different software applications on the workstations that are connected to the network."

__Current Status__: IMPLEMENTED

As stated previously, DOC is using TrackIt to monitor both of its hardware and software inventories. Furthermore, DOC staff can generate reports periodically on all the software installed on DOCNET. Therefore, we consider Recommendation #4 implemented.

__Previous Recommendation #5__: DOC's "Manager of PC Support [should] use the information from the application tracking software, once it has been installed, to ensure that all software applications are properly licensed."

Previous Agency Response: "MIS is in the process of purchasing the appropriate number of licenses to make all our systems 'legal'."

Current Status: NOT IMPLEMENTED

Although DOC provided a report, generated from TrackIt, which listed all the software packages on its network and identified the licensed software bought in 2001, we found 71 software packages installed on DOCNET that are not licensed. Accordingly, we consider Recommendation #5 not implemented.

****

PREVIOUS FINDING: "DOCNET protection against computer virus is inadequate: while anti-virus software is installed on DOCNET workstations, it is not installed on DOCNET servers."

Previous Recommendation #6: "We recommend that DOC's Manager of PC Support and its Manager of LAN Support purchase and install anti-virus software that offers a combination of server and client protection."

Previous Agency Response: "MIS is currently investigating appropriate anti-virus software, and will purchase and install it as soon as a selection is made."

Current Status: IMPLEMENTED

DOC purchased anti-virus software from Network Associates, Inc., that has been installed on DOCNET and provides security anti-virus protection for both servers and clients. Accordingly, we consider Recommendation #6 implemented.

****

PREVIOUS FINDING: "We found nine user accounts with OPEN VMS authorization privileges."

Previous Recommendation #7: "We recommend that DOC's Data Center Manager and its System Programming Manager review all the accounts with special privileges, that they determine the number of accounts that can be removed, and that they remove these accounts."

Previous Agency Response: "MIS will comply with this recommendation."

Current Status: **NOT IMPLEMENTED**

We reviewed a list of 1,500 user accounts with access to DOCNET, and found 16 users who had access privileges to the Open VMS Operating System, which is on the DOCNET servers. Nine of the 16 active user accounts in Open VMS have the "all" privilege, which is the highest level of privileges to the Open VMS Operating System. With the "all" privilege, the user can disregard any protection of the data, and add or delete user accounts on DOCNET. Users with this privilege have the potential to control the system. Such level access should be granted to the data center manager, the system manager, and the night shift manager only. Accordingly, we consider Recommendation #7 not implemented.

NEW FINDINGS

Security Architecture Proposal Submitted

DOC submitted a Security Architecture Proposal to DOI, in accordance with DOI system security standards. DOI approved the proposal, and DOC is in the process of developing related forms and documentation.

Inventory Control Procedures

DOC's inventory control policies and procedures were promulgated on April 30, 1997. The DOI *Standards for Inventory Control and Management*, § 6, states: "Agency management is responsible for ensuring that there are policies and procedures and that these are updated [emphasis added] . . . ." Although DOI does not provide guidance on when updates are to occur, we believe that DOC should review its procedures and update them whenever changes have been made to the computer inventory system.

Recommendations

DOC should:

1. Record new computer equipment on FMS, and remove retired or obsolete equipment from FMS.

DOC Response: "With regard to the PC and printer purchase, DOC will comply with the audit recommendation by entering the information in the Fixed Asset Inventory System Report. With regard to salvaged items that are still on the Report, the Department, in cooperation with the Agency Chief Contracting Officer, will ensure that these items are taken off of the report."

2. Review all accounts with special privileges to the Open VMS Operating System to determine the number of accounts that can be removed, and remove these accounts.

DOC Response: "Of the 16 accounts, nine are generated or required for the functionality of the operating system or layered products. To remove any privileges from these accounts would render the systems non-functional. For these nine accounts it is clear that removal of the privileges is not possible.

"Moreover, it is important to note that (unlike the IBM world) not all users who have the 'all' privilege have all of the privileges. This parameter is misleading, i.e., the users actually have less power than the 'all' parameter setting suggests."

Auditor Comment: As stated in the report, the "all" user privilege should be assigned only to the data center manager, the system manager, and the night shift manager. This will provide ample coverage to address problems and prevent system downtime while ensuring system security. In addition, our review of these nine accounts after receiving DOC's response indicated that seven accounts were not assigned to an actual user; consequently, more than one user may have access to each of these accounts. This poses a security risk since DOC would be unable to link unauthorized or improper use to specific users. Therefore, we repeat our recommendation that DOC review these accounts to determine which accounts can be removed and then either delete these accounts or assign them to specific users.

3. Create a written policy that prevents the illegal copying or pirating of its software and software documentation and that prevents the installation of illegal software on the network.

DOC Response: "DOC as an agency is fully licensed, and DOC follows the policy of only installing licensed software. The ' . . . software packages installed on the DOCNET that are not licensed' are installed by users. Most PCs on the network currently run Windows 95, which does not allow us to lock-down the PCs. As a result the users can install unauthorized and unlicensed (by DOC) software. We are migrating to Windows 2000, which allows us to lock-down the PCs, thereby denying users the ability to install software. The migration to Windows 2000 will be completed by December, at which time all unauthorized software will be removed. We are in the process of purchasing the Microsoft Enterprise Agreement to ensure that we will always be compliant with Microsoft licensing requirements. MIS will comply [with this recommendation]."

4. Review its software inventory and delete all illegal software.

DOC Response: "MIS will comply [with this recommendation]."

5. Review and update its inventory policies and procedures.

DOC Response: "MIS will comply [with this recommendation]."

The City of New York

NEW YORK CITY DEPARTMENT OF CORRECTIO
William J. Fraser, Commissione
Office of the Commissione

60 Hudson Stree
New York, NY 1001

646 • 248 • 121
Fax 646 • 248 • 121

June 11, 2002

Roger D. Liwer
Executive Deputy Comptroller
The City of New York
Office of the Comptroller
1 Center Street – Room 530
New York, New York 10007-2341

Dear Mr. Liwer:

Attached is this agency's response to your "Follow-up Audit of the Department of Correction Local Area Network", number 7F02-162. We have responded to those items that you have indicated are "Not Implemented". We have addressed each of your findings and recommendations.

If you have any further questions regarding this response, please contact Douglas E. Waldmann, Deputy Commissioner, Technical Development and Project Management at (646) 248-1607.

Sincerely,

William J Fraser
WILLIAM J. FRASER

c: Gary M. Lanigan, First Deputy Commissioner
John J. Antonelli, Deputy Commissioner, Administration
Leroy Grant, Chief of Inspectional Services and Compliance Division
Douglas E. Waldmann, Deputy Commissioner, Technical Development & Project Management

Department of Correction
Response to
Follow-up Audit of the
Department of Correction Local Area Network
7F02-162
May 30, 2002

This report addresses Follow-up Audit findings that are indicated as "Not Implemented". Each section contains the report finding, followed by our response – "Department of Correction Response".

REGARDING RECOMMENDATION # 3 (page 6 - 7 of the report)

Previous Findings: "New computer equipment is not recorded on the IFMS Fixed Assets accounting report."

Recommendation #3: "We recommend that DOC's Purchasing Manager follow the proper procedures to ensure that new equipment is added and maintained on the IFMS [Integrated Financial Management System] Fixed Assets System." He should also ensure that retired/obsolete equipment is removed from the IFMS Fixed Assets Systems."

Previous Agency Response: "MIS does follow the proper procedures with regards to the IFMS Fixed Assets System….The equipment [used for DOCNET] consists of items, largely PCs and printers, all of which cost less than $15,000 each. Moreover the minimum useful life of a PC, is by no stretch of the imagination, five years. Therefore this equipment does not belong on the IFMS Fixed Assets System."

Current Status: NOT IMPLEMENTED

DOC purchased 119 personal computers, at a cost of $208,514 and 125 printers, at a cost of $98,942, during 2001. These items, which were purchased through the Capital Budget, were not listed in the IFMS Fixed Asset Inventory System Report. We also noted that equipment reported in the previous audit (purchased in 1984 and 1985) that is reportedly no longer in use is still listed on the Fixed Asset Inventory Report. Accordingly, we consider Recommendation #3 not implemented.

Department of Correction Response: With regard to the PC and printer purchase, DOC will comply with the audit recommendation by entering the information in the Fixed Asset Inventory System Report. With regard to salvaged items that are still on the Report, the Department, in cooperation with the Agency Chief Contracting Officer, will ensure that these items are taken off of the report.

****

REGARDING RECOMMENDATION # 5 (page 8 of the report)

Previous Recommendation #5: DOC's "Manager of PC Support [should] use the information from the application tracking software, once it has been installed, to ensure that all software applications are properly licensed."

Previous Agency's Response: "MIS is in the process of purchasing the appropriate number of licenses to make all our systems legal."

Current Status: NOT IMPLEMENTED

Although DOC provided a report, generated from TrackIt, which listed all the software packages on its network and identified the licensed software bought in 2001, we found 71 software packages installed on DOCNET that are not licensed. Accordingly, we consider Recommendation #5 not implemented.

Department of Correction Response: DOC as an agency is fully licensed, and DOC follows the policy of only installing licensed software. The "...software packages installed on the DOCNET that are not licensed" are installed by the users. Most PCs on the network currently run Windows 95, which does not allow us to lock-down the PCs. As a result the users can install unauthorized and unlicensed (by DOC) software. We are migrating to Windows 2000, which allows us to lock-down the PCs, thereby denying users the ability to install software. The migration to Windows 2000 will be completed by December, at which time all unauthorized software will be removed. We are in the process of purchasing the Microsoft Enterprise Agreement to ensure that we will always be compliant with Microsoft licensing requirements.

****

REGARDING RECOMMENDATION # 7 (page 8 – 9 of the report)

Previous Findings: "We found nine user accounts with OPEN VMS authorized privileges."

Previous Recommendation #7: "We recommend that DOC's Data Center Manager and its System Programming Manager review all the accounts with special privileges, that they determine the number of accounts that can be removed, and that they remove these accounts."

Previous Agency Response: "MIS will comply with this recommendation."

Current Status: NOT IMPLEMENTED

We reviewed a list of 1,500 user accounts with access to DOCNET, and found 16 users who had access privileges to the Open VMS Operating System, which is on the DOCNET servers. Nine of the 16 active user accounts in Open VMS have the "all" privilege, which is the highest level of privileges in the Open VMS Operation System. With the "all" privilege, the user can disregard any protection of the data, and add or delete user accounts on DOCNET. Users with this privilege have the potential to control the system. Such level access should be granted to the data center manager, the system manager, and the night shift manager only. Accordingly, we consider Recommendation #7 not implemented.

Department of Correction Response: Of the 16 accounts, nine are generated or required for the functionality of the operating system or layered products. To remove any privileges from these accounts would render the systems non-functional. For these nine accounts it is clear that removal of the privileges is not possible.

The remaining seven actual accounts are used to perform production or managerial functions on the cluster. Because of the 7 x 24 nature of our operations, and because of the mission-critical publicsafety nature of our complex systems, it is important that we have staff available with who can perform their necessary work from home without delay. These accounts must have these privileges to do their job. To remove the privileges would impede either managerial tasks or job functionality, and would reduce our ability to respond to problems. The result would be greater downtime. Moreover, it is important to note that (unlike the IBM world) not all users who have the "all" privilege have all of the privileges. This parameter is misleading, i.e., the users actually have less power than the "all" parameter setting suggests.

NEW FINDINGS

Inventory Control Procedures

DOC's inventory control policies and procedures were promulgated on April 30, 1997. The DOI Standards for Inventory Control and Management, paragraph 6, states: "Agency management is responsible for ensuring that there are policies and procedures and that these are updated [emphasis added]…." Although DOI does not provide guidance on when updates are to occur, we believe that DOC should review its procedures and update them whenever changes have been made to the computer inventory system.

Recommendations

DOC should:

Record new computer equipment on IFMS, and remove retired or obsolete equipment from IFMS.

Review all accounts with special privileges to the Open VMS Operating System to determine the number of accounts that can be removed, and remove these accounts.

Create a written policy that prevents the illegal copying or pirating of its software and software documentation and that prevents the installation of illegal software on the network.

Review its software inventory and delete all illegal software.

Review and update its inventory policies and procedures.

Department of Correction Response:

This item was addressed above.

This item was addressed above.

MIS will comply.

MIS will comply.

MIS will comply.