



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

WILLIAM C. THOMPSON, JR.
Comptroller

**Audit Report on the
Department of Environmental Protection
Data Center**

7A02-069

May 21, 2002

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

**Audit Report on the
Department of Environmental Protection
Data Center**

7A02-069

EXECUTIVE SUMMARY

Background

The New York City Department of Environmental Protection (DEP) supplies 1.35 billion gallons of drinking water to more than seven million City residents and to one million water users in four upstate counties. DEP daily treats an average of 1.27 billion gallons of wastewater at 23 wastewater treatment facilities. It finances the maintenance, growth, and rehabilitation of the water and sewer systems through revenue from water and sewer fees paid by consumers. Finally, DEP enforces provisions of the City Administrative Code that regulate air, noise, hazardous materials, and asbestos abatement.

The DEP central data center, located at DEP headquarters, supports the main local area network (LAN). The central data center also connects to smaller bureau data centers within the agency, such as those for the Bureaus of Wastewater Treatment, Environmental Engineering, and Water and Sewer Operations. Users can connect to LAN applications that include the Automated Complaint System and the Facilities Information Tracking system.

The DEP Management Information System division (MIS) is responsible for developing, maintaining, and supporting application software and for operating the data center.

Objectives

Our audit objectives were:

- To review the adequacy of the central data center's physical and system security.

- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with Comptroller's Directive #18 (Directive 18), the City Department of Investigation's (DOI) *Standards for Inventory Control and Management*, and the *Federal Information Processing Standards* (FIPS).

Scope and Methodology

Audit fieldwork began in July 2001 and ended on January 2, 2002. To achieve our objectives we:

- Interviewed DEP personnel;
- Conducted a walk-through of the central data center;
- Reviewed and analyzed data security controls;
- Reviewed DEP's *Computing and Networking Policy and Procedures*;
- Evaluated DEP's network disaster recovery controls;
- Reviewed DEP's *Internet Security Architecture Plan*;
- Tested DEP compliance with FIPS;
- Tested DEP compliance with Directive 18; and
- Tested DEP compliance with the DOI *Standards for Inventory Control and Management*.

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

Results in Brief

The DEP central data center is not in compliance with certain requirements of Directive 18, FIPS, and DOI inventory control policies. Specifically, the data center is not monitored 24 hours a day, and a fire extinguishing system has not been installed. In addition, the log-on access of 81 inactive or former employees has not been disabled, and DEP has no procedures to document, review, and follow up on network-security access violations. Moreover, proper inventory procedures have not been established to ensure that all computer equipment is accounted for, and DEP has not installed filtering software to reduce the risk of users' accessing inappropriate web sites.

Recommendations

The report contains 14 recommendations, the most critical of which are listed below. DEP management should:

- Test the data center's UPS equipment regularly.
- Identify and terminate inactive user accounts.
- Require that all server passwords be changed every 42 days.
- Eliminate unnecessary generic accounts.
- Complete and formally approve a disaster recovery plan (for the network and software). Once the plan is completed and approved, DEP should periodically test it and document the results to ensure that the plan functions as intended and is adequate to quickly resume computer operations without material loss of data.
- Install a security filtering system or firewall on all PCs with Internet access.

Agency Response

The matters covered in this report were discussed with officials from the DEP during and at the conclusion of this audit. A preliminary draft report was sent to DEP officials and discussed at an exit conference held on April 11, 2002. On April 23, 2002, we submitted a draft report to DEP officials with a request for comments. We received a written response DEP on May 7, 2002. DEP generally agreed with the audit's finding and recommendations and has started implementing some of the recommendations.

The full text of DEP comments is included as an Addendum to this report.

Table of Contents

	Page
INTRODUCTION	1
Background.....	1
Objectives	1
Scope and Methodology.....	2
Agency Response	2
FINDINGS AND RECOMMENDATIONS.....	3
Noncompliance with Directive 18 and FIPS.....	3
Weakness in Physical Security.....	3
UPS Equipment not Tested Periodically.....	3
System Access.....	4
Log-in Access of Inactive and Former Employees not Adequately Controlled	4
DEP Allows Users Unlimited Log-in Attempts	4
MIS Administrative Access	4
Shared Passwords.....	4
Excessive Number of Generic Accounts	5
Security Violations not Adequately Monitored.....	5
Disaster Recovery Plan.....	5
Inventory Weakness.....	6
Internet Connectivity.....	6
RECOMMENDATIONS.....	7
ADDENDUM - Agency Response	

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

**Audit of the
Department of Environmental Protection
Data Center**

7A02-069

INTRODUCTION

Background

The New York City Department of Environmental Protection (DEP) supplies 1.35 billion gallons of drinking water to more than seven million City residents and to one million water users in four upstate counties. DEP daily treats an average of 1.27 billion gallons of wastewater at 23 wastewater treatment facilities. It finances the maintenance, growth, and rehabilitation of the water and sewer systems through revenue from water and sewer fees paid by consumers. Finally, DEP enforces provisions of the City Administrative Code that regulate air, noise, hazardous materials, and asbestos abatement.

The DEP central data center, located at DEP headquarters, supports the main local area network (LAN). The central data center also connects to smaller bureau data centers within the agency, such as those for the Bureaus of Wastewater Treatment, Environmental Engineering, and Water and Sewer Operations. Users can connect to LAN applications that include the Automated Complaint System and the Facilities Information Tracking system.

The DEP Management Information System division (MIS) is responsible for developing, maintaining, and supporting application software and for operating the data center.

Objectives

Our audit objectives were:

- To review the adequacy of the central data center's physical and system security.
- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with Comptroller's Directive #18 (Directive 18), the

City Department of Investigation's (DOI) *Standards for Inventory Control and Management*, and the *Federal Information Processing Standards (FIPS)*.

Scope and Methodology

Audit fieldwork began in July 2001 and ended on January 2, 2002. To achieve our objectives we:

- Interviewed DEP personnel;
- Conducted a walk-through of the central data center;
- Reviewed and analyzed data security controls;
- Reviewed DEP's *Computing and Networking Policy and Procedures*;
- Evaluated DEP's network disaster recovery controls;
- Reviewed DEP's *Internet Security Architecture Plan*;
- Tested DEP compliance with FIPS;
- Tested DEP compliance with Directive 18; and
- Tested DEP compliance with the DOI *Standards for Inventory Control and Management*.

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 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 the DEP during and at the conclusion of this audit. A preliminary draft report was sent to DEP officials and discussed at an exit conference held on April 11, 2002. On April 23, 2002, we submitted a draft report to DEP officials with a request for comments. We received a written response DEP on May 7, 2002. DEP generally agreed with the audit's finding and recommendations and has started implementing some of the recommendations.

The full text of DEP comments is included as an Addendum to this report.

**OFFICE OF THE COMPTROLLER
NEW YORK CITY**

DATE FILED: May 21, 2002

FINDINGS AND RECOMMENDATIONS

The DEP central data center is not in compliance with certain requirements of Directive 18, FIPS, and DOI inventory control policies. Specifically, the data center is not monitored 24 hours a day, and a fire extinguishing system has not been installed. In addition, the log-on access of 81 inactive or former employees has not been disabled, and DEP has no procedures to document, review, and follow up on network-security access violations. Moreover, proper inventory procedures have not been established to ensure that all computer equipment is accounted for, and DEP has not installed filtering software to reduce the risk of users' accessing inappropriate web sites or downloading viruses.

Noncompliance with Directive 18 and FIPS

Weaknesses in Physical Security

DEP has not installed a security system to continuously monitor the data center. Data centers are normally equipped with surveillance cameras or alarm systems that can be used to monitor data center activity and alert management when unauthorized individuals attempt to access the data center. In addition, the entrance door to the data center can be opened with a regular door key that can easily be copied. Moreover, although the data center had portable fire extinguishers and smoke detectors, it was not equipped with a fire extinguishing system. Directive 18, § 7.4, states:

“Controls for limited access spaces housing the agency’s most sensitive equipment, typically a computer room, data center or hubsite, include: (1) Entry restriction only to authorized personnel. Available systems vary greatly in sophistication, ranging from simple key card, to biometric access devices, some can deny access to even authorized personnel during specific periods, some can record the identity, for later review, of all persons entering and leaving, some will sound audible intruder alarms. (2) Humidity and temperature detection devices with alarms, smoke detectors. (3) Fire extinguishing systems.”

Physical security controls such as swipe cards, surveillance cameras, alarm systems, and fire extinguishing systems represent the most basic protection for unauthorized access to the data center and for the prevention of theft or destruction of equipment.

UPS Equipment not Tested Periodically

In accordance with Directive 18, DEP installed uninterruptable power supply (UPS) units at the data center to keep equipment running or shut it down in an orderly fashion if electric power is cut off for any reason. However, DEP does not test its UPS systems periodically, in accordance with FIPS 31 § 3.1, which states: “appropriate steps should be taken to assure that the quality and reliability of electric power will satisfy the needs of the facility.”

System Access

Log-in Access of Inactive and Former Employees not Adequately Controlled

DEP has not deleted network log-in access privileges for its former employees. In October 2001, 81 inactive or former employees had active user accounts, although the City Payroll Management System database showed that these employees were no longer employed, were terminated, or were on extended leave. The failure to delete these user accounts is contrary to Directive 18, § 8.1.2, which requires “deactivation of inactive user accounts and accounts for employees whose services have terminated.”

Users Allowed Unlimited Log-in Attempts

DEP’s system does lock out users who have made five unsuccessful attempts to log-on to the system; however, after each set of five unsuccessful attempts, an individual need wait only 10 minutes before trying to log-on again. FIPS 112 states:

“The number of allowed password entry attempts (retries after an incorrect password entry) shall be limited to a number selected by the Security Officer. The response to exceeding the maximum number of retries shall be specified by the Security Officer.”

If the number of log-on attempts is not restricted, there is an increased risk of unauthorized access to the system.

MIS Administrative Access

Eighteen MIS administrators (domain administrators) have special privileges to create, delete, and modify user and group information. Giving this level of access to so many people increases the risk of damage, removal, or alteration of critical files or programs, which could ultimately impair network and agency operations.

Shared Passwords

Unique local passwords should be assigned to each local server to limit user access to the local servers, thereby minimizing the risk of unauthorized access to critical files and programs. However, 16 of DEP’s 23 local servers have the same password. Thus if an unauthorized user gained access to one of these servers, that individual would have access to all 16 servers. In addition, two other local servers had passwords that were set to expire in 49,710 days; the other 21 servers required the passwords to be changed every 42 days. Directive 18 states, “password management includes insuring that users are forced to change passwords periodically.”

Excessive Number of Generic Accounts

As of October 4, 2001, there were 476 generic log-on accounts on the system. These accounts included ones with names as simple as “User 1,” “User 2,” and “Auditor.” Generic accounts allow multiple users to log on to the system under one user name. By including so many generic accounts in the system, DEP cannot track individual user activity or prevent unauthorized access to sensitive system data.

Security Violations not Adequately Monitored

DEP has no procedures to monitor security violations on its network. Such procedures, if followed, would help the agency identify patterns of violations and ensure that when needed, proper controls are instituted to prevent unauthorized access to the system. These procedures would be easy to implement, since Windows NT has a built-in function that allows for the tracking of security violations. Directive 18, § 11.5, states:

“A record of the physical and logical security violations detected by software controls and other monitoring procedures must be reported to senior management. The most serious security violations should be reported to executive management. A review of security violations will highlight unresolved problems or weaknesses in internal controls and may show patterns of failure and abuse requiring remedial action.”

Disaster Recovery Plan

DEP's disaster recovery plan is not complete, not formally approved, and not periodically tested. Directive 18 states that agencies should establish a written disaster recovery plan that should be a “formal plan for the recovery of agency operations and the continuation of business after a disruption due to a major loss of computer processing capability.” Specifically, DEP's disaster plan does not include critical information, such as the names, telephone numbers, and specific responsibilities of each individual to be contacted in case of a disaster; the order in which systems are to be reinstated; a list of equipment and software supply agreements; and provision for an alternative-processing site.

Inventory Weaknesses

DEP does not maintain a complete and accurate list of all computer equipment installed at the agency. Specifically, the existing list does not always include a complete description of the equipment, such as the type of equipment, the manufacturer, and the model number. In fact, for 1,148 pieces of equipment, the description column on the inventory records was left blank, making it difficult to account for the equipment.¹ DEP did not perform an annual inventory of its installed computer equipment. Directive 18 states “physical inventories should, at a minimum, be conducted annually to insure that actual equipment matches the inventory records. All discrepancies must be resolved.”

Also, DEP does not maintain an up-to-date inventory of its software licenses. Directive 18 § 4.1 0.1 states:

“The first step in evaluating the information processing environment is to . . . identify the automated systems and software products that support each business function, including the numbers and types of software licenses owned and in use.”

Maintaining an up-to-date list of software licenses is important to DEP’s ability to track software use and to ensure that only licensed software is being used on agency systems.

Moreover, DEP does not maintain inventory records of new computer equipment that has not yet been installed. Accordingly, DEP inventory practices do not comply, even at the basic level, with the DOI *Standards for Inventory Control and Management*, which lists inventory guidelines for all City agencies. These guidelines require that agencies maintain inventory records to deter and detect the loss of inventory. Specifically, the guidelines state that: “records present a complete picture of the ‘who, what, when, and why’ of a transaction from initiation to completion. Records demonstrating less than this are not adequate.” The guidelines further state that “a perpetual inventory system is established to maintain an up-to-date count of all items in the inventory. A running balance of the goods on hand is maintained by the timely recording of the quantities of incoming and outgoing orders.” Finally, the standards require annual physical counts to confirm the accuracy of the perpetual records.

Internet Connectivity

Under DOI System Security Standards, City agencies that plan to provide agency-wide Internet access must submit a proposal to DOI for approval. DEP submitted its Internet Security Architecture Plan to DOI and received approval in a letter dated June 12, 2001. According to the approved plan, DEP will establish outbound Internet access for its staff and inbound Internet access for the public. The functions that will be available are in the early stages of development.

¹ Normally, we compare the Agency inventory list to the Fixed Asset Inventory Report on the Integrated Financial Management System’s (IFMS) for capital fund purchases made prior to July 1, 1999 and to the Financial Management System’s (FMS) Fixed Asset Inventory Report for capital fund purchases subsequent to June 30, 1999. The starting point for such a test is the agency’s list of equipment. However, since DEP’s list was missing critical information, the review of the IFMS and FMS reports could not be performed.

Currently, DEP provides limited Internet access to its staff through 33 stand-alone computers. Internet access authorization is based on an individual's need to perform specific job functions. The agency's computers, however, have virus protection but lack a security filtering system or firewall to prevent user access to unauthorized Internet sites. Directive 18, § 9.1, requires that security software or firewall software be used to control and track access to Internet sites.

Recommendations

We recommend that DEP:

1. Restrict access to the central data center to authorized personnel by installing a swipe card system or other access control device.

Agency Response: "The entrance to the data center is equipped with a swipe card system and is part of the facility-wide access control system. Inside the data center, a key-lock door additionally protects the Agency's servers. While DEP disagrees with the auditors's observation that the data center is protected by the key-lock only, DEP agrees that the existing swipe card system provides access to the main data center area to more staff than is desirable. This is due to limitations of the access control system. That system is being upgraded and will permit the assignment of access privileges to a more restrictive set of individuals. The Department is also relocating the servers area within the data center and will continue to provide additional access control to that area."

2. Install surveillance cameras or an alarm system to monitor the facility 24 hours a day, seven days a week.

Agency response: "A surveillance camera has historically been used to monitor the entrance to the data center, but DEP agrees with the auditor's recommendation that cameras also be used within the area. DEP has already installed a camera inside the main room and will locate additional cameras to specifically monitor the server and network areas. The layout of the data center is being redesigned and the additional cameras will be installed as that work progresses."

3. Install a fire extinguishing system in the data center.

Agency response: "The Department agrees with the auditor's observation that the data center is protected by a fire alarm system and portable extinguishers, but has no automatic extinguishing system. The Department is planning to have a fire safety evaluation performed of the area by a professional consultant who will be asked to recommend an appropriate automatic extinguishing system. The Department plans to act upon the consultant study to procure and install an automatically activated system."

4. Test the data center's UPS equipment regularly.

Agency response: "The data center's UPS is activated regularly during normal operations in response to utility power dips and has been fully exercised during Y2K testing and subsequent planned shutdowns of power for internal building work. The UPS is equipped with internal monitoring and status sensors and is checked on a regular basis. However, the Department agrees that full-load testing of the unit has not been regularly performed and will do so."

5. Identify and terminate inactive user accounts.

Agency response: "On a monthly basis, the central MIS unit reviews the data center domain account list to identify non-deleted accounts for separated employees. Of 81 accounts identified in the audit, 42 were accounts of employees whose services had ceased subsequent to the start of the month (September 2001). Of the 39 accounts predating September, one employee was in fact actively employed and all but 2 were last documented in non-termination classes (Leave of Absence, Maternity Leave, Sick Leave, etc.). The Department agrees that domain accounts should be disabled for employees who are on extended leave and will include this review as part of the central MIS monthly examination. The accounts identified in the audit have been disabled or deleted as appropriate."

6. Lock out system users after five unsuccessful attempts to log-on to the system.

Agency response: "The historical temporary lockout of accounts after unsuccessful login attempts provides a high degree of protection against unauthorized network access given the time that would be required to break a user password. However, the Department agrees that locking accounts until proactively reactivated by a domain administrator will further enhance security and has already implemented this change."

7. Review the appropriateness of permitting as many as 18 MIS personnel to have unlimited network access.

Agency response: "Agency MIS functions are largely decentralized among central MIS and operating Bureau technical staff. The number of network administrators is a function of that decentralization. While the number of administrators required in a decentralized environment is larger than necessary in a centralized one, the Department agrees that the number can be reduced and is evaluating administrative privileges across the network to limit such access to as few personnel as necessary."

8. Assign a unique password to each server.

Agency response: “The Department agrees with this recommendation and is assigning unique passwords to data center member server local administrator accounts.”

9. Require that all local server passwords be changed every 42 days.

Agency response: “The Department agrees with this recommendation and has modified the expiration of passwords for the two servers.”

10. Eliminate unnecessary generic accounts.

Agency response: “Domain accounts not associated with specific individuals include those automatically created by system and network software to support system services, those established for employee training purposes, special workstation needs such as shared scanners/printers, and other operating requirements. The Department agrees that the number of these accounts is larger than desirable and is evaluating all ‘generic’ accounts to reduce this number to the minimum necessary.”

11. Establish formal procedures to document and report network access violations, and review and follow up on all reported access violations.

Agency response: “The Department agrees with this recommendation and plans to implement new security hardware, software and formal policies/procedures in Fiscal 2003 that comply with Citywide security infrastructure guidelines issued by the Departments of Investigations and Information Technology and Telecommunications. This project, already submitted to the City’s Technology Steering Committee and based upon a plan approved by DOI/DoITT, will enable the Department to provide network based Internet access and will augment existing internal security controls.”

12. Complete and formally approve a disaster recovery plan (for the network and software). Once the plan is completed and approved, DEP should periodically test it and document the results to ensure that the plan functions as intended and is adequate to quickly resume computer operations without material loss of data.

Agency response: “The Department had prepared planning documents for contingency operations under system failure conditions and for network and systems restoration from failure. These have been tested. The Department agrees that the existing plans do not fully cover disaster contingencies and is preparing a disaster-specific planning document that will be formally approved and periodically tested.”

13. Maintain a complete and accurate list of all computer equipment (including new equipment not yet installed) and software licenses and perform an annual inventory to ensure that the physical equipment matches the inventory records.

Agency response: “The Department instituted a centralized inventory system in Fiscal 2001 and has been working to improve its inventory functions. Annual physical inventories are performed but the Department agrees that an effective front-end covering new purchases and installations has not yet been implemented for the central system. Central MIS is working to implement a procedure for capturing hardware and software information from procurement through retirement for agency information assets and plans to have implemented this procedure by the end of summer 2002. Pending implementation of this inventory control improvement, the Department is using a combination of central inventory data and Bureau inventory reports to account for its inventory additions.”

14. Install a security filtering system or firewall on all PCs with Internet access.

Agency response: “The Department agrees that Internet access must be controlled and plans to implement site and content filtering as part of its network security infrastructure project. Based upon an already approved security plan, this project is expected to be completed in Fiscal 2003 and will limit user access to resources specified in central firewall policies. In the interim, stand-alone PC’s used to access the Internet already have virus protection software and the Department is reviewing the effectiveness of stand-alone firewall products that could be used until the planned security infrastructure is implemented.”



**Department of
Environmental
Protection**

59-17 Junction Boulevard
Flushing, New York
718-373-5108

**Christopher O. Ward
Commissioner**

**Louis J. Tazzi
Deputy Commissioner
Bureau of Management
and Budget**

Tel: (718) 595-3403
Fax: (718) 595-3437



(718) DEP-HELP

May 7, 2002

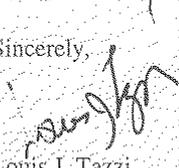
Roger D. Liwer
Assistant Comptroller for Audits
The City of New York Office of the Comptroller
1 Centre Street, Room 1100 North
New York, New York 10007-2341

**Re: Audit Number 7A02-069 - Audit Report on the Department of
Environmental Protection Data Center**

Dear Mr. Liwer:

Thank you for the opportunity to comment on the above referenced audit. We appreciate the opportunity to respond to the draft report and our comments on each recommendation are attached.

Sincerely,


Louis J. Tazzi

Comptroller's cc: Christopher O. Ward, Dennis McClain

Dist: Diana Chapin
Charles Sturcken
Louis Tazzi
Anne McCarthy
Mark Hoffer
Geoffrey Ryan
Rosemarie Subasic
Frank Munari
Purnell Lancaster (Operations)

Audit Number 7A02-069: Audit Report on the DEP's Data Center

Recommendation 1:

Restrict access to the central data center to authorized personnel by installing a swipe card system or other access control device.

Agency Response:

The entrance to the data center is equipped with a swipe card system and is part of the facility-wide access control system. Inside the data center, a key-lock door additionally protects the Agency's servers. While DEP disagrees with the auditor's observation that the data center is protected by the key-lock only, DEP agrees that the existing swipe card system provides access to the main data center area to more staff than is desirable. This is due to limitations of the access control system. That system is being upgraded and will permit the assignment of access privileges to a more restrictive set of individuals. The Department is also relocating the server area within the data center and will continue to provide additional access control to that area.

Recommendation 2:

Install surveillance cameras or an alarm system to monitor the facility 24 hours a day, seven days a week.

Agency Response:

A surveillance camera has historically been used to monitor the entrance to the data center, but DEP agrees with the auditor's recommendation that cameras also be used within the area. DEP has already installed a camera inside the main room and will locate additional cameras to specifically monitor the server and network areas. The layout of the data center is being redesigned and the additional cameras will be installed as that work progresses.

Recommendation 3:

Install a fire extinguishing system in the data center.

Agency Response:

The Department agrees with the auditor's observation that the data center is protected by a fire alarm system and portable extinguishers, but has no automatic extinguishing system. The Department is planning to have a fire safety evaluation performed of the area by a professional consultant who will be asked to recommend an appropriate automatic extinguishing system. The Department plans to act upon the consultant study to procure and install an automatically activated system.

Audit Number 7A02-069: Audit Report on the DEP's Data Center

Recommendation 4:

Test the Data Center's UPS equipment regularly.

Agency Response:

The data center's UPS is activated regularly during normal operations in response to utility power dips and has been fully exercised during Y2K testing and subsequent planned shutdowns of power for internal building work. The UPS is equipped with internal monitoring and status sensors and is checked on a regular basis. However, the Department agrees that full-load testing of the unit has not been regularly performed and will do so.

Recommendation 5:

Identify and terminate inactive user accounts.

Agency Response:

On a monthly basis, the central MIS unit reviews the data center domain account list to identify non-deleted accounts for separated employees. Of 81 accounts identified in the audit, 42 were accounts of employees whose services had ceased subsequent to the start of the month (September 2001). Of the 39 accounts predating September, one employee was in fact actively employed and all but 2 were last documented in non-termination classes (Leave of Absence, Maternity Leave, Sick Leave, etc.). The Department agrees that domain accounts should be disabled for use for employees who are on extended leave and will include this review as part of the central MIS monthly examination. The accounts identified in the audit have been disabled or deleted as appropriate.

Recommendation 6:

Lock out system users after five unsuccessful attempts to log on to the system.

Agency Response:

The historical temporary lockout of accounts after unsuccessful login attempts provides a high degree of protection against unauthorized network access given the time that would be required to break a user password. However, the Department agrees that locking accounts until proactively reactivated by a domain administrator will further enhance security and has already implemented this change.

Audit Number 7A02-069: Audit Report on the DEP's Data Center

Recommendation 7:

Review the appropriateness of permitting as many as 18 MIS personnel to have unlimited network access.

Agency Response:

Agency MIS functions are largely decentralized among central MIS and operating Bureau technical staff. The number of network administrators is a function of that decentralization. While the number of administrators required in a decentralized environment is larger than necessary in a centralized one, the Department agrees that the number can be reduced and is evaluating administrative privileges across the network to limit such access to as few personnel as necessary.

Recommendation 8:

Assign a unique password to each server.

Agency Response:

The Department agrees with this recommendation and is assigning unique passwords to data center member server local administrator accounts.

Recommendation 9:

Require that all local server passwords be changed every 42 days.

Agency Response:

The Department agrees with this recommendation and has modified the expiration of passwords for the two servers.

Recommendation 10:

Eliminate unnecessary generic accounts.

Agency Response:

Domain accounts not associated with specific individuals include those automatically created by system and network software to support system services, those established for employee training purposes, special workstation needs such as shared scanners/printers, and other operating requirements. The Department agrees that the number of these accounts is larger than desirable and is evaluating all "generic" accounts to reduce this number to the minimum necessary.

Audit Number 7A02-069: Audit Report on the DEP's Data Center

Recommendation 11:

Establish formal procedures to document and report network access violations, and review and follow up on all reported access violations.

Agency Response:

The Department agrees with this recommendation and plans to implement new security hardware, software and formal policies/procedures in Fiscal 2003 that comply with Citywide security infrastructure guidelines issued by the Departments of Investigations and Information Technology and Telecommunications. This project, already submitted to the City's Technology Steering Committee and based upon a plan approved by DOI/DoITT, will enable the Department to provide network based Internet access and will augment existing internal security controls.

Recommendation 12:

Complete and formally approve a disaster recovery plan (for the network and software). Once the plan is completed and approved, DEP should periodically test it and document the results to ensure that the plan functions as intended and is adequate to quickly resume computer operations without material loss of data.

Agency Response:

The Department had prepared planning documents for contingency operations under system failure conditions and for network and systems restoration from failure. These have been tested. The Department agrees that the existing plans do not fully cover disaster contingencies and is preparing a disaster-specific planning document that will be formally approved and periodically tested.

Recommendation 13:

Maintain a complete and accurate list of all computer equipment (including new equipment not yet installed) and software licenses and perform an annual inventory to ensure that the physical equipment matches the inventory records.

Agency Response:

The Department instituted a centralized inventory system in Fiscal 2001 and has been working to improve its inventory functions. Annual physical inventories are performed but the Department agrees that an effective front-end covering new purchases and installations has not yet been implemented for the central system. Central MIS is working to implement a procedure for capturing hardware and software information from procurement through retirement for agency information assets and plans to have implemented this procedure by the end of summer 2002.

Audit Number 7A02-069: Audit Report on the DEP's Data Center

Pending implementation of this inventory control improvement, the Department is using a combination of central inventory data and Bureau inventory reports to account for its inventory additions.

Recommendation 14:

Install a security filtering system or firewall on all PC's with Internet access.

Agency Response:

The Department agrees that Internet access must be controlled and plans to implement site and content filtering as part of its network security infrastructure project. Based upon an already approved security plan, this project is expected to be completed in Fiscal 2003 and will limit user access to resources specified in central firewall policies. In the interim, stand-alone PC's used to access the Internet already have virus protection software and the Department is reviewing the effectiveness of stand-alone firewall products that could be used until the planned security infrastructure is implemented.