AUDIT REPORT

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

Follow-up Audit Report on the Department of Environmental Protection Data Center

7F04-065

March 19, 2004

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 responsibilities of the Comptroller contained in Chapter 5, § 93, of the New York City Charter, my office has reviewed the implementation status of 14 recommendations made in a previous audit entitled, *Audit Report on the Department of Environmental Protection Data Center* (Audit # 7A02-069, issued May 21, 2002). The results of our audit, which are presented in this report, have been discussed with Environmental Protection officials, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that City agencies have adequate controls in place to protect their equipment and records from inappropriate access and use.

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

William C. Thompson, Jr.

WCT/GR

Report: **7F04-065**
Filed: **March 19, 2004**

Table of Contents

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

Follow-up Audit Report on the Department of Environmental Protection Data Center

7F 04-065

AUDIT REPORT IN BRIEF

This follow-up audit determined whether the New York City Department of Environmental Protection (DEP) implemented the 14 recommendations made in a previous audit of its data center. In this report, we discuss the 14 recommendations from the prior audit in detail, as well as the current status of each recommendation.

In Fiscal Year 2002, our office conducted an audit of DEP's physical security procedures, system security procedures, disaster recovery plans, and operational procedures for protecting its computer equipment inventory and information. The audit also determined whether DEP complied with Comptroller's Internal Control and Accountability Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems*; the Department of Investigation's (DOI) *Standards for Inventory Control and Management*; DOI's Information Security Directive 4.4; and applicable Federal Information Processing Standards (FIPS).

The previous audit found a number of weaknesses, including that the data center was not monitored 24 hours a day, and that a fire extinguishing system had not been installed. In addition, that audit noted that log-on access of 81 inactive or former employees had not been disabled, and that DEP had no procedures to document and review network-security access violations. Moreover, DEP did not follow proper inventory procedures to ensure that all its computer equipment was accounted for, and it had no formal disaster recovery plan for its critical systems.

Audit Findings and Conclusions

DEP implemented nine and did not implement five of the 14 recommendations made in the previous audit. In this follow-up audit, we found that DEP made some improvements in its data center physical and system security—a swipe-card system has been installed to restrict access to the data center and a surveillance camera has been installed to monitor the data center 24 hours a day,

seven days a week; the data center's Uninterruptable Power Supply (UPS) is being tested periodically; and the agency has terminated log-in access for inactive users and improved its system access controls. However, the center still lacks a fire extinguishing system, there are generic log-on accounts that still need to be eliminated, and a formal procedure has not been created that requires that the access-violation report be reviewed. In addition, DEP has not developed a formal disaster recovery plan to ensure business continuity, and its computer equipment inventory records are not kept up-to-date.

Audit Recommendations

To address the issues that still exist, we recommend that DEP:

- Install a fire extinguishing system in the data center.
- Reevaluate current generic log-on accounts and eliminate any that are unnecessary.
- Establish formal procedures to document and report network access violations, and review and follow up on all reported access violations.
- 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.
- Maintain a complete and accurate list of all computer equipment and perform an annual inventory to ensure that all equipment items on hand are included on the inventory records.

INTRODUCTION

Background

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 treats an average of 1.27 billion gallons of wastewater daily at 23 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. It enforces provisions of the City Administrative Code that regulate air, noise, hazardous materials, and asbestos abatement.

The central data center supports DEP's 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.

DEP's Information Technology (IT) division is responsible for developing, maintaining, and supporting application software and for operating the data center. DEP has several smaller IT divisions that are responsible for specific operational bureaus within the agency. During calendar year 2003, DEP began to centralize its IT divisions and to formalize IT security procedures and policies.

Objectives

The objective of this audit was to determine whether DEP implemented the 14 recommendations made in an earlier report, *Audit Report on the Department of Environmental Protection Data Center* (Audit # 7A02-069, issued May 21, 2002).

Scope and Methodology

This audit covered the period August through November 2003. To determine the implementation status of the recommendations, we:

- toured the data center and noted the current physical security measures in place;
- interviewed DEP personnel;
- reviewed and analyzed data security controls;
- reviewed and analyzed DEP security procedures for remote dial-in-access, password assignment, LAN, Internet, and mainframe access, and the tracking of user activity;
- tested DEP compliance with Comptroller's Directive 18 and applicable FIPS and DOI standards.

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 DEP officials 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 February 11, 2004. On February 12, 2004, we submitted a draft report to DEP officials with a request for comments. We received a written response from DEP on March 3, 2004. In its response, DEP indicated that it agrees with the report's recommendations stating that it "is continuing its efforts to implement the remaining 5 [recommendations]." With regard to implementing the remaining recommendations, DEP stated:

"The challenge to full implementation of those recommendations. . . is heightened by the distributed and/or decentralized computing environment that has historically characterized computer operations within DEP. The Department has also been addressing these broader issues through initiatives that include the hiring of an Assistant Commissioner for Information Technology and establishment of the Office of Information Technology (in Fiscal 2003) to centrally oversee, coordinate and/or manage all IT development and operations within the Department. While helping to improve the overall effectiveness and efficiency of IT operations within the Department, augmented control is also reinforcing the Agency's efforts to improve overall systems security hardware, software and data."

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

RESULTS OF FOLLOW-UP AUDIT

Previous Finding: "The entrance to the data center is not monitored 24 hours a day, and a fire extinguishing system has not been installed . . .. In addition, the entrance door to the data center can be opened with a regular door key that can be easily copied."

Previous Recommendation #1: **"**Restrict access to the central data center to authorized personnel by installing a swipe card system or other access control device."

Previous DEP 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' 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."

Current Status: IMPLEMENTED

DEP has installed a swipe-card access system for its data center. Access is restricted to authorized personnel. Only the DEP security division can activate swipe cards. Therefore, we consider Recommendation #1 implemented.

Previous Recommendation #2: **"**Install surveillance cameras or an alarm system to monitor the facility 24 hours a day, seven days a week."

Previous DEP 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."

Current Status: IMPLEMENTED

DEP installed a surveillance camera to monitor the data center 24 hours a day, seven days a week. Therefore, we consider Recommendation #2 implemented.

Previous Recommendation #3: **"**Install a fire extinguishing system in the data center."

Previous DEP 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."

Current Status: NOT IMPLEMENTED

DEP still has not installed a fire extinguishing system in the data center. In addition, contrary to its response to the prior audit, DEP did not hire a consultant to perform a fire safety evaluation. According to the Assistant Commissioner for Information Technology, a request for a fire extinguishing system has been submitted to DEP's budget committee, but it has not yet been approved. Therefore, we consider Recommendation #3 not implemented.

Previous Finding: "DEP does not test its UPS system periodically, in accordance with FIPS 31 §3.1."

Previous Recommendation #4: "Test the data center's UPS equipment regularly."

Previous DEP 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."

Current Status: IMPLEMENTED

DEP tested its UPS equipment in March 2003. In addition, during the citywide blackout in August 2003, the UPS system provided sufficient power for the IT division to safely shut down its servers with a minimal loss of data. Therefore, we consider Recommendation #4 implemented.

Previous Finding: "DEP has not deleted network log-in access privileges for its former employees."

Previous Recommendation #5: "Identify and terminate inactive user accounts."

Previous DEP 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."

Current Status: IMPLEMENTED

DEP's password security system has been reprogrammed to cancel inactive passwords after ninety days. In addition, we confirmed that all active passwords on DEP's system are assigned to current employees. Therefore, we consider Recommendation #5 implemented.

Previous Finding: "Users allowed unlimited log-in attempts—DEP's system does lock out users who have made five unsuccessful 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."

Previous Recommendation #6: "Lock out system users after five unsuccessful attempts to log-on to the system."

Previous DEP 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."

Current Status: IMPLEMENTED

Currently, users are locked out of DEP's system after five unsuccessful log-on attempts. In addition, all system lockouts require that the system administrator reset and reactivate user passwords. Therefore, we consider Recommendation #6 implemented.

Previous Finding: "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."

Previous Recommendation #7: "Review the appropriateness of permitting as many as 18 MIS personnel to have unlimited network access."

Previous DEP 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."

Current Status: IMPLEMENTED

DEP has reduced the number of domain system administrators with unlimited network access to four. Therefore, we consider Recommendation #7 implemented.

Previous Finding: "Sixteen of DEP's 23 local servers have the same password." In addition, two of the 23 local servers' passwords were set to expire in 49,710 days; the other 21 servers required that passwords be changed every 42 days.

Previous Recommendation #8: "Assign a unique password to each server."

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

Previous Recommendation #9: "Require that all local server passwords be changed every 42 days."

Previous DEP Response: "The Department agrees with this recommendation and has modified the expiration of passwords for the two servers."

Current Status: IMPLEMENTED

DEP has assigned a unique password to each server, and all passwords are set to expire every 42 days. Therefore, we consider Recommendations #8 and #9 implemented.

Previous Finding: "There are an excessive number of generic accounts on the system." The audit found 476 generic log-on accounts in DEP's computer environment. Generic accounts allow multiple users access to the system through one user name, thereby making it difficult for the agency to track individual user activity or prevent unauthorized access to sensitive system data.

Previous Recommendation #10: "Eliminate unnecessary generic accounts."

Previous DEP 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."

Current Status: NOT IMPLEMENTED

Although DEP eliminated 99 of the 476 generic accounts, there is still an excessive number of generic accounts in its computer environment. Therefore, we consider Recommendation #10 not implemented.

Previous Finding: "DEP has no procedures to monitor security violations on its network.

Previous Recommendation #11: "Establish formal procedures to document and report network access violations, and review and follow up on all reported access violations."

Previous DEP 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."

Current Status: NOT IMPLEMENTED

DEP still does not have formal procedures in place to monitor security violations on its network. Although DEP officials receive access-violation reports, there are no agency policies and

procedures in place ensuring that these reports are reviewed and violations are followed up. Therefore, we consider Recommendation #11 not implemented.

Previous Finding: "DEP's disaster recovery plan is not complete, not formally approved, and not periodically tested." Its plan did not include critical information, such as contact person's name, telephone numbers, specific responsibilities of each individual, and the order in which systems are to be reinstated.

Previous 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."

Previous DEP 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."

Current Status: NOT IMPLEMENTED

DEP still does not have a complete, formally approved, and periodically tested disaster recovery plan. Therefore, we consider Recommendation #12 not implemented.

Previous Finding: "DEP does not maintain a complete and accurate list of all computer equipment installed at the agency." In addition, "DEP did not perform an annual inventory of its installed computer equipment . . . 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 a basic level, with DOI *Standards for Inventory Control and Management*, which lists inventory guidelines for all City agencies."

Previous 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."

Previous DEP 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."

Current Status: NOT IMPLEMENTED

DEP still does not maintain a complete and accurate list of its computer inventory. According to DEP's Assistant Commissioner of Information Technology, the agency's inventory list has not been updated for at least two years. In fact, we noted that the inventory list contained many obsolete items and did not include recently acquired equipment. Therefore, we consider Recommendation #13 not implemented.

Previous Finding: "The agency's computers have virus protection but lack a security filtering system or firewall to prevent user access to unauthorized Internet sites."

Previous Recommendation #14: "Install a security filtering system or firewall on all PCs with Internet access."

Previous DEP 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."

Current Status: IMPLEMENTED

The agency's computers now have a security filtering system to prevent user access to unauthorized Internet sites. Therefore, we consider Recommendation #14 implemented.

RECOMMENDATIONS

To address the issues that still exist, we recommend that the Department of Environmental Protection:

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

DEP Response: "The Department agrees with this recommendation. The data center has been inspected by DEP and other City engineers and funds have been requested to install a fire extinguishing system. This project was originally combined with a larger facility upgrade that includes installation of emergency power generating equipment for the data

center and network. These projects have been separated to expedite the approval of funds and design/installation of the extinguishing system. In the interim, the Department has installed additional alarm sensors in the data center to provide improved protection."

2. Reevaluate current generic log-on accounts and eliminate any that are unnecessary.

DEP Response: "The Department agrees with this recommendation and, as such, had already eliminated 21 percent of the non-named accounts. Of the accounts remaining, most are system services accounts, training accounts, and technical support accounts. All system services accounts are being reviewed to identify an individual responsible party and the assignment of those accounts is being recorded in the domain directory. Passwords for student accounts are being changed after each class to prevent unauthorized use. Accounts used by technicians are being evaluated for continued necessity and are eliminated when no longer needed. Individual responsibility for these accounts is also being recorded in the domain directory. The auditors' original recommendation was directed to "shared" accounts. These have been virtually eliminated and the Department plans to have no accounts used by more than one person in its directory by end of Fiscal 2004."

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

DEP Response: "The Department agrees with this recommendation. In Fiscal 2003 the Department began implementing new security hardware and software resources to identify network access violations and is reorganizing staff to ensure timely review, reporting, and follow up for identified violations."

4. 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.

DEP Response: "The Department agrees with this recommendation and is continuing its efforts to fully develop a formal disaster recovery plan. While contact information, vendor support information, and operating contingencies have been prepared and maintained, the Department has not yet completed the design and implementation of an alternate site network operations center and associated testing. In conjunction with other emergency operations and incident management enhancements, the Department is finalizing its site selection and configuration plans. These will then be incorporated into the formal recovery plan."

5. Maintain a complete and accurate list of all computer equipment and perform an annual inventory to ensure that all equipment items on hand are included on the inventory records.

DEP Response: "The Department agrees with this recommendation and is continuing its effort to implement an adequate inventory system that monitors and protects hardware and

software assets throughout the full procurement/disposition life cycle. As reported previously, the Agency has implemented a bar-code tagging and physical inventory system. However, the shortcomings of the process include timeliness of update (previously on an annual cycle), and logistical problems associated with controlling resources ordered, delivered, allocated, used, and disposed in a largely decentralized computing environment. Addressing these issues, the Department has already centralized its network operations and is expanding central control over desktop support, applications and software, and IT procurement. DEP is also implementing helpdesk and security software that will largely automate the physical inventory process and provide timely information for equipment reallocations."

The City of New York

Department of Environmental Protection

59-17 Junction Boulevard
Flushing, New York
11373-5108

Christopher O. Ward
Commissioner

Robert E. Cucinotta
Assistant Commissioner

Office of Information Technology

Tel (718) 595-7805
Fax (718 595-4065
rcucinotta@dep.nyc.gov

March 1, 2004

William C. Thompson, Jr.
New York City Comptroller
Office of the Comptroller
1 Centre Street
New York, NY 10007-2341

RE: Follow-up Audit Report on the Department of Environmental Protection Data Center 7F04-065

Dear Mr. Thompson:

We are in receipt of the above referenced draft audit report and would like to thank you for the opportunity to comment. Since the time of the original data center audit, the Department has implemented 9 of the 14 recommendations made therein and is continuing its efforts to implement the remaining 5. These are in varying phases of implementation as described below in detail.

The challenge to full implementation of those recommendations not yet implemented is heightened by the distributed and/or decentralized computing environment that has historically characterized computer operations within DEP. The Department has also been addressing these broader issues through initiatives that include the hiring of an Assistant Commissioner for Information Technology and establishment of the Office of Information Technology (in Fiscal 2003) to centrally oversee, coordinate and/or manage all IT development and operations within the Department. While helping to improve the overall effectiveness and efficiency of IT operations within the Department, augmented control is also reinforcing the Agency's efforts to improve overall systems security for hardware, software and data.

As in the past, we thank you for the valuable information external reviews of Agency operations provide in our efforts to improve services and the overall structure of controls.

Sincerely,

Robert Cucinotta,
Assistant Commissioner, Information Technology

NEW YORK CITY DEPARTMENT OF ENVIRONMENTAL PROTECTION
DEP
www.nyc.gov/dep
(718) DEP-HELP

Audit Recommendation 1. (Previous Recommendation #3):

Install a fire extinguishing system in the data center.

Department Response:

The Department agrees with this recommendation. The data center has been inspected by DEP and other City engineers and funds have been requested to install a fire extinguishing system. This project was originally combined with a larger facility upgrade that includes installation of emergency power generating equipment for the data center and network. These projects have been separated to expedite the approval of funds and design/installation of the extinguishing system. In the interim, the Department has installed additional alarm sensors in the data center to provide improved protection.

Audit Recommendation 2. (Previous Recommendation #10):

Eliminate unnecessary generic accounts.

Department Response:

The Department agrees with this recommendation and, as such, had already eliminated 21 percent of the non-named accounts. Of the accounts remaining, most are system services accounts, training accounts, and technical support accounts. All system services accounts are being reviewed to identify an individual responsible party and the assignment of those accounts is being recorded in the domain directory. Passwords for student accounts are being changed after each class to prevent unauthorized use. Accounts used by technicians are being evaluated for continued necessity and are eliminated when no longer needed. Individual responsibility for these accounts is also being recorded in the domain directory. The auditors' original recommendation was directed to "shared" accounts. These have been virtually eliminated and the Department plans to have no accounts used by more than one person in its directory by end of Fiscal 2004.

Audit Recommendation 3. (Previous Recommendation #11):

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

Department Response:

The Department agrees with this recommendation. In Fiscal 2003 the Department began implementing new security hardware and software resources to identify network access violations and is reorganizing staff to ensure timely review, reporting, and follow up for identified violations.

Audit Recommendation 4. (previous 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.

Department Response:

The Department agrees with this recommendation and is continuing its efforts to fully develop a formal disaster recovery plan. While contact information, vendor support information, and operating contingencies have been prepared and maintained, the Department has not yet completed the design and implementation of an alternate site network operations center and associated testing. In conjunction with other emergency operations and incident management enhancements, the Department is finalizing its site selection and configuration plans. These will then be incorporated into the formal recovery plan.

Audit Recommendation 5. (Previous 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.

Department Response:

The Department agrees with this recommendation and is continuing its efforts to implement an adequate inventory system that monitors and protects hardware and software assets throughout the full procurement/disposition life cycle. As reported previously, the Agency has implemented a bar-code tagging and physical inventory system. However, the shortcomings of the process include timeliness of update (previously on an annual cycle), and logistical problems associated with controlling resources ordered, delivered, allocated, used, and disposed in a largely decentralized computing environment. Addressing these issues, the Department has already centralized its network operations and is expanding central control over desktop support, applications and software, and IT procurement. DEP is also implementing help-desk and security software that will largely automate the physical inventory process and provide timely information for equipment reallocations.