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 Buildings Data Center

7A02-062

April 2, 2002

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

Audit Report on the Department of Buildings Data Center

7A02-062

EXECUTIVE SUMMARY

Background

The Department of Buildings (DOB) oversees building construction and alteration in New York City (the City). The agency also enforces building and electrical codes, zoning resolutions, the New York State multiple dwelling law, and energy, safety, labor, and other laws related to construction activity. DOB inspects construction and electrical, plumbing, and elevator installations. Its inspectors respond to complaints about the structural integrity of buildings. In addition, DOB issues licenses to individuals in construction-related trades, such as plumbers, electricians, welders, boiler operators, riggers, and hoisting machine operators.

DOB uses mainframe computers to provide information on permits, violations, complaints, ownership, and geographical and landmark data. Its Building Information System (BIS) is accessible through public information terminals. DOB is currently working with the Department of Information Technology and Telecommunications (DoITT) to provide an Internet access feature on the BIS database. This will enable the public to view property profiles and complaint resolution status, and to learn whether particular individuals are licensed by DOB. The agency also uses personal computers (PCs), which give access to its Local Area Network and Wide Area Network (LAN/WAN).

DOB's Information Technology (IT) department is responsible for developing and supporting application software and for operating the Data Center.

Objectives

Our audit objectives were:

- To review the adequacy of the Data Center's physical and system security.

- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with the standards in Comptroller's Directive 18 (Directive 18) and the Federal Information Processing Standards (FIPS).

Scope and Methodology

We conducted our fieldwork from July through December 2001. To achieve our objectives we:

- Interviewed DOB personnel;
- Conducted walk-throughs of the Data Center;
- Reviewed and analyzed data security controls;
- Reviewed DOB's *Computing and Networking Policy and Procedures*;
- Reviewed and evaluated DOB's *Network Disaster Recovery Plan*;
- Reviewed DOB's *Internet Security Architecture Plan*; and
- Tested DOB's compliance with Directive 18.

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

DOB's Data Center is not in compliance with certain physical security requirements of Directive 18 and of FIPS. Specifically, the Data Center is not monitored on a 24-hour basis, smoke detectors and a fire extinguishing system have not been installed, and the Data Center is not adequately protected from a loss of power. Moreover, DOB has no automated time-out feature installed on its network. The log-in access of 117 inactive employees has not been disabled, and 18 former employees' mainframe accounts have not been deleted. Furthermore, DOB has not established formal procedures to document, review, and follow up network-security access violations. DOB has no written policies in place to ensure that only appropriate and authorized changes are made to its application and system software. Finally, DOB still has not completed its disaster recovery plan and had it formally approved by DOB management and periodically tested.

Major Recommendations

This audit made 13 recommendations; the major recommendations are that DOB should:

- Install an emergency cut-off switch to shut down power in the event of an emergency.
- Install a backup generator at the Data Center.
- Install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system.
- Have its Personnel Department immediately advise IT of those employees leaving or terminated from the agency. IT should then promptly delete these accounts.
- Identify and terminate inactive user accounts.
- Complete and formally approve its *Network Disaster Recovery Plan*. Once the Plan is completed and approved, DOB should periodically test it and document the test results to ensure that the plan functions as intended, and is adequate to quickly resume computer operations without material loss of data.
- Secure an alternative-processing site for resuming computer operations in the event of a disaster.

Agency Response

The matters covered in this report were discussed with officials from DOB during and at the conclusion of this audit. A preliminary draft was sent to DOB officials and discussed at an exit conference held on March 5, 2002. On March 6, 2002, we submitted a draft report to DOB officials with a request for comments. We received a written response from DOB on March 20, 2002. DOB generally agreed with the audit's findings and recommendations, stating that "the Department is in the process, or has implemented all of the 13 recommendations contained in the report." DOB also stated that "the content of these 13 recommendations has helped the Department review and strengthen our procedures."

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

Table of Contents

INTRODUCTION ……. 1

Background ……..……... 1

Objectives ……...…… 1

Scope and Methodology …… 2

Agency Response …….. 2

FINDINGS AND RECOMMENDATIONS …….. 3

Recommendations ……. 7

ADDENDUM - DOB Response

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

Audit Report on the Department of Buildings Data Center

7A02-062

INTRODUCTION

Background

The Department of Buildings (DOB) oversees building construction and alteration in New York City (the City). The agency also enforces building and electrical codes, zoning resolutions, the New York State multiple dwelling law, and energy, safety, labor, and other laws related to construction activity. DOB inspects construction and electrical, plumbing, and elevator installations. Its inspectors respond to complaints about the structural integrity of buildings. In addition, DOB issues licenses to individuals in construction-related trades, such as plumbers, electricians, welders, boiler operators, riggers, and hoisting machine operators.

DOB uses mainframe computers to provide information on permits, violations, complaints, ownership, and geographical and landmark data. Its Building Information System (BIS) is accessible through public information terminals. DOB is currently working with the Department of Information Technology and Telecommunications (DoITT) to provide an Internet access feature on the BIS database. This will enable the public to view property profiles and complaint resolution status, and to learn whether particular individuals are licensed by DOB. The agency also uses personal computers (PCs), which give access to its Local Area Network and Wide Area Network (LAN/WAN).

DOB's Information Technology (IT) department is responsible for developing and supporting application software and for operating the Data Center.

Objectives

Our audit objectives were:

- To review the adequacy of the Data Center's physical and system security.

- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with the standards in Comptroller's Directive 18 (Directive 18) and the Federal Information Processing Standards (FIPS).

Scope and Methodology

We conducted our fieldwork from July through December 2001. To achieve our objectives we:

- Interviewed DOB personnel;
- Conducted walk-throughs of the Data Center;
- Reviewed and analyzed data security controls;
- Reviewed DOB's *Computing and Networking Policy and Procedures*;
- Reviewed and evaluated DOB's *Network Disaster Recovery Plan*;
- Reviewed DOB's *Internet Security Architecture Plan*; and
- Tested DOB's compliance with Directive 18.

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 DOB during and at the conclusion of this audit. A preliminary draft was sent to DOB officials and discussed at an exit conference held on March 5, 2002. On March 6, 2002, we submitted a draft report to DOB officials with a request for comments. We received a written response from DOB on March 20, 2002. DOB generally agreed with the audit's findings and recommendations, stating that: "the Department is in the process, or has implemented all of the 13 recommendations contained in the report." DOB also stated that "the content of these 13 recommendations has helped the Department review and strengthen our procedures."

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

OFFICE OF THE COMPTROLLER
NEW YORK CITY

DATE FILED: April 2, 2002

FINDINGS AND RECOMMENDATIONS

DOB's Data Center is not in compliance with certain physical security requirements of Directive 18 and of FIPS. Specifically, the Data Center is not monitored on a 24-hour basis, smoke detectors and a fire extinguishing system have not been installed, and the Data Center is not adequately protected from a loss of power. Moreover, DOB has no automated time-out feature installed on its network. The log-in access of 117 inactive employees has not been disabled, and 18 former employees' mainframe accounts have not been deleted. Furthermore, DOB has not established formal procedures to document, review, and follow up network-security access violations. DOB has no written policies in place to ensure that only appropriate and authorized changes are made to its application and system software. Finally, DOB still has not completed its disaster recovery plan and had it formally approved by DOB management and periodically tested.

Noncompliance with Directive 18 and FIPS

DOB has not installed a security system to monitor the Data Center continuously. 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. Moreover, although the Data Center has portable fire extinguishers, it is not equipped with smoke detectors and 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 surveillance cameras and alarm systems are the most basic protection against unauthorized access to the Data Center and theft or destruction of equipment. DOB officials installed two smoke detectors in the Data Center after we discussed this issue with them. Still, the Data Center does not comply with § 7.4 of Directive 18.

In addition, Directive 18, § 7.2, requires that the Data Center have uninterruptable power supply (UPS) units to "keep equipment running, and/or shut it down in an orderly fashion, when electric power is cut off for any reason." DOB has UPS units that can keep Data Center equipment running for 30 to 45 minutes, but has not installed an emergency cut-off switch and backup power generator at the Data Center. FIPS Publication 31 states:

> "In the event of a fire, flooding or other emergency, it is important to be able to shut off electric power quickly, easily and selectively. First, one can use the power-off switch on the individual unit. However, one should remember that the power cable and circuitry . . . are still energized. These can be de-energized by manually tripping the branch circuit breaker at the distribution panel."

FIPS Publication 31 further states that on-site power generation can be installed to guard against power outages that last more than 30 to 45 minutes (the capacity of the UPS units). DOB officials told us they are planning to move the Data Center to a new location and will purchase a backup generator at the new site. However, DOB has no scheduled date for the move. The current Data Center will remain vulnerable to prolonged power blackouts until this condition is resolved.

Network not Equipped with Automatic Time-out Feature

DOB's network is not equipped with a time-out feature that automatically locks workstations after extended periods of inactivity. Instead, DOB's workstations are individually equipped with the feature. However, this is not an adequate approach for controlling access, since all employees may not activate the feature. When they do not, unauthorized individuals can access sensitive agency data after employees leave their workstations. Directive 18, § 8.1, states that "a simple access control is the use of a time out feature that automatically logs off an end user workstation if no activity is detected after a pre-specified time."

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

DOB has not deleted mainframe log-in access privileges for its former employees. In November 2001, we found that 18 former employees still had active user accounts for 1 month to 13 years after leaving the agency. These individuals were listed on the City Payroll Management System (PMS) database as no longer employed, terminated, or on separation leave. Not deleting these user accounts is contrary to Directive 18, § 8.1.2, which requires "(3) Deactivation of inactive user accounts and accounts for employees whose services have terminated."

In January 2002, DOB provided us with a revised list of mainframe user accounts that purportedly corrected the problem. However, according to the list, 4 of the 18 former DOB employees still had log-in access to the mainframe.

In addition, 117 of the 750 network user accounts and passwords (including 2 of the 18 cited above) were unused for periods ranging from 1 month to 9 years. Although inactive for long periods, these accounts and passwords were not disabled. This was in violation of § 8.1.2 of Directive 18, which states that "active password management includes . . . deactivation of inactive user accounts." DOB also violated its *Computing and Network Policy and Procedures*, which state:

> "Network accounts inactive for 30 days will be disabled (account will remain available but no one will be able to use that account to login to the network). If a request to enable the account is not received in the next 60 days it will be deleted. Users who will be on leave or otherwise will not be using their account for 90 days or more should inform Network Engineering. Their account will then be disabled but not deleted to ensure there is no unauthorized use during the period of inactivity."

Security Violations are not Adequately Monitored

DoITT is responsible for disaster recovery and system security for DOB's mainframe computer. DoITT informs the agency of security violations via e-mail. However, the e-mails do not provide detailed information on each incident, which should include the number of unauthorized log-in attempts as well as the files, programs, or data for which access was attempted. Nor does DOB have procedures to ensure that security violations on its network are recorded, documented, and reviewed. Such procedures would help the agency identify patterns of violations and help ensure that proper controls are instituted to prevent unauthorized access to the system. 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."

Undocumented Changes to User Accounts

DOB does not document when new accounts or changes to user accounts are requested and approved. Its *Computing and Networking Policy and Procedures* states that "requests for new Network Accounts must be authorized by a unit head and the request must come from the Unit Head or their authorized representative. . . . New or Changed Network Account Information should be entered on the Computer Network Services Request Form."

In a written response to our inquiry for copies of *Computer Network Service Request Forms*, DOB stated that "The Department of Buildings being a small agency with approx. 695 employees, the Data Center would allow e-mail from the individual supervisor requesting any action be taken by the Data Center on behalf of the employee. If the supervisor can e-mail the Network supervisor, then that proves the authenticity." Nevertheless, DOB officials did not provide copies of any e-mail requests to the Data Center. Such documentation would provide evidence that all changes made to network information were authorized.

Inadequate Program Change Procedures

DOB does not document when changes to application and system software are requested and approved. DOB has no written policies in place to ensure that only appropriate, authorized changes are made to its application and system software. Agency officials told us that users were allowed to submit their change requests by e-mail. IT does not log-in user change requests when received, does not keep the requests in electronic or hard copy form, does not assign individual job numbers to the requests, and does not maintain formal change-control logs to document the outcome of the requests. Therefore, we could not determine whether only appropriate and authorized changes were made to DOB's application and system software. Program change management involves modifying program, data, and files. All changes or modifications to system software should be completely documented, tested, and approved.

Directive 18, § 9.3, states: "A change control policy is necessary to insure that only appropriate, authorized changes are made to application and system software." In that regard, § 9.3.1, states that the:

> "Elements of a change control program include: A formal approval and review process that ensures that changes to application and operating system programs and data are not made unless explicitly authorized by appropriate agency personnel."

Without effective program change management DOB risks unauthorized or unnecessary program changes to its system software.

Disaster Recovery Plan

DOB has no complete, formally approved, and periodically tested disaster recovery plan. In conformance with Directive 18, a *Network Disaster Recovery Plan* contains procedures for three levels of events—catastrophic disaster, limited disaster, and minor disaster. Directive 18, § 10.1, states that "In developing business continuation plans, agencies must consider separately scenarios involving the loss of a data center, satellite office, or other critical points of failure in the agency's information processing environment." However, DOB's plan dated July 2001, states that it is a "Work in Progress" document that should not be considered a final disaster recovery plan. The plan's catastrophic disaster procedures adequately plan for total loss of the network command center. However, the limited disaster and minor disaster procedures for loss of one or more servers or a remote server room, and for the loss of a database, web page(s) or loss of enterprise or departmental files, have not been completed.

Moreover, DOB has no alternative-processing site to bring the system up and running in the event of emergencies or system failure. DOB could reestablish limited operations at one of its remote sites. However, this would be only a temporary and limited solution, because these sites do not have all of the equipment needed to run all DOB applications and prolonged use of the remote site would have a negative impact on the remote site's ability to perform its primary functions.

Internet Connectivity

Under Department of Investigation (DOI) System Security Standards, agencies that plan to provide agency-wide Internet access must submit a proposal to DOI for approval. DOB submitted its *Internet Security Architecture Plan* to DOI and received approval in a letter dated May 22, 2001. According to the approved plan, DOB will implement Internet access in two phases. At present, DOB is in the first phase, which will establish outbound Internet access for its staff. Phase two will provide for inbound Internet access. The applications and transactions that will be available are currently in the early stages of development.

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

security software or firewall software be used to control and track access to Internet sites. DOB employees could, therefore, gain access to inappropriate Internet sites, and also download viruses that could be transferred to the agency's network.

DOB started testing its new agency-wide Internet access connection in December 2001. All previous Internet access (stand-alone computers) will be disabled when testing is completed. DOB's new Internet policy requires that its employees fill out an application to gain agency-wide Internet access. Currently, Internet access has been set up for 33 DOB employees. According to DOB officials, by the end of February 2002 all DOB employees who have completed the application will have Internet access.

Recommendations

We recommend that DOB officials:

1. Install surveillance cameras or an alarm system in the Data Center to monitor the facility on a 24 hour, 7-day a week basis.

   DOB Response: "The Department is in the process of relocating to 280 Broadway and equipment has already been delivered to this location. The move of the Data Center, we anticipate, should take place 12 weeks from March 18, 2002. Senior management is presently in talks with DCAS regarding the building security and the installation of surveillance cameras, in particular the installation of surveillance cameras in the Data Center. It is anticipated that there will be 24/7 coverage by security guards."

2. Install a fire extinguishing system in the Data Center.

   DOB Response: "A fire extinguishing system has been installed throughout the Department's new location at 280 Broadway, including the Data Center."

3. Install an emergency cut-off switch to shut down power in the event of an emergency.

   DOB Response: "The Department does have an emergency cut-off switch. A distribution panel is assigned to the Data Center. In the event of an emergency, the Department shuts down each component of its Data Center systematically, whether there is electricity or not. We do have UPS units that keep Data Center equipment running for 30 to 45 minutes. Sufficient time the Department thinks, before manually tripping the branch circuit breaker and the master switch. At 280 Broadway, the Department will make one change from its procedure at 60 Hudson Street, concerning its emergency cut-off switch. One UPS unit with the capacity to keep the equipment running for 23 minutes will control all the Department's components."

   Auditor Comment: DOB's audit coordinator stated that it was not until after the draft report was issued that the agency realized that the data center had an emergency cut-off switch. However, the emergency cut-off switch was never tested to ensure that it would function properly in an emergency situation.

4. Install a backup generator at the Data Center.

   DOB Response: "There is interrupted power supply at the Department's present location, 60 Hudson Street. At 280 Broadway the Department will have uninterrupted power, supplied from the street. Since there [are] significant issues surrounding the purchase of a backup generator, the Department is currently analyzing the feasibility of this. Senior managers will meet to discuss purchasing a backup generator at the Data Center."

5. Install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system.

   DOB Response: "The Department agrees with this recommendation and has started implementing it throughout the Department."

6. Have its Personnel Department immediately advise IT of those employees leaving or terminated from the agency. IT should then promptly delete these accounts.

   DOB Response: "The Department agrees with this recommendation and is in the process of establishing written procedures regarding deleting accounts for those employees leaving or terminated from the agency. In addition, the Department's Personnel Unit will be required to advise the IT Unit regarding employees separation dates."

7. Identify and terminate inactive user accounts.

   DOB Response: "In addition to the Agency Response (#6) above, it is the Department current policy of disabling a password after 30 days of inactive use and removing expired passwords after 90 days of inactive use. The Department is making every effort to ensure that the IT unit is following its policy."

8. Establish formal procedures with DoITT to document and report mainframe access violations, and review and follow up on all reported access violations.

   DOB Response: "DOB agrees with this recommendation and is currently working with DoITT to establish written procedures regarding DOB mainframe access violations."

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

   DOB Response: "DOB agrees with this recommendation and is currently working to establish formal procedures to document and report network access violations. The Department will also review and follow-up on all reported access violations."

10. Ensure that changes to user accounts are made in accordance with its *Computing and Networking Policy and Procedures*. In this regard, DOB should document when changes to user accounts are requested and approved.

    DOB Response: "The agency agrees with the above recommendation and the IT Unit will take additional steps to ensure that any change to users accounts are documented as indicated in the agency Computing and Networking Policy and Procedures."

11. Establish written policies to ensure that only appropriate, authorized changes are made to its application and system software. In this regard, IT officials should document the requests received and the changes IT makes in response to the requests.

    DOB Response: "The agency's IT Unit is in the process of establishing written policies to alleviate unauthorized changes to the Department's application and system software. In addition, the IT Unit will take additional steps to ensure that changes to users account are documented."

12. Complete and formally approve its *Network Disaster Recovery Plan*. Once the Plan is completed and approved, DOB should periodically test it and document the test results to ensure that the plan functions as intended, and is adequate to quickly resume computer operations without material loss of data.

    DOB Response: "The Department will devote additional resources to the completion of its Network Disaster Recovery Plan. Once completed the Department will ensure compliance."

13. Secure an alternative-processing site for resuming computer operations in the event of a disaster.

    DOB Response: "The Department is in the process of installing new network equipment and servers at its new location at 280 Broadway. DOB plans to use the existing network equipment at its present location (60 Hudson Street) and set up an alternative-processing site, most likely in one of our borough offices, in the event of an emergency. The

Department's Senior Managers will meet to discuss the location of an emergency site or other viable alternatives."

NEW YORK CITY
DEPARTMENT OF BUILDINGS
EXECUTIVE OFFICES
60 HUDSON STREET, NEW YORK, N.Y. 10013-3394
website:NYC.gov/buildings
Ronny Livian, P.E., Acting Commissioner

Richard N. Bernard
Deputy Director/Chief of Management Audits
Program & Management Analysis
(646) 248-8035
(646) 248-8065 Fax
Email: richardb@buildings.nyc.gov

March 19, 2002

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

Re: Audit Report on the Department of Buildings Data Center 7A02-062

Dear Mr. Liwer:

Thank you for the opportunity to comment on the above referenced draft audit report. I am also pleased to note as described further below, that the Department is in the process, or has implemented all of the 13 recommendations contained in the report.

As your report notes, the objectives of the Office of the Comptroller were as follows:

- To review the adequacy of the Data Center's physical and system security.
- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with standards in Comptroller's Directive 18 (Directive 18) and the Federal Information Processing Standards (FIPS).

The content of these 13 recommendations has helped the Department review and strengthen our procedures. Attached is the Department's response to these specific recommendations. If you have any questions or require any clarification you may reach me at the telephone numbers and e-mail address listed above.

Sincerely,

Richard N. Bernard

cc: Patricia J. Lancaster, R.A.
Ronny A. Livian, P.E.
Patricia Ketterer
Mark Topping
Fred Badalamenti
Peggy Rose Viera, MOO
Fred D'Alo
Matti Friedman
Encl.

Auditor Recommendation #1:

Install surveillance cameras or an alarm system in the Data Center to monitor the facility on a 24 hour, 7-day a week basis.

Agency Response:

The Department is in the process of relocating to 280 Broadway and equipment has already been delivered to this location. The move of the Data Center, we anticipate, should take place 12 weeks from March 18, 2002. Senior management is presently in talks with DCAS regarding the building security and the installation of surveillance cameras, in particular the installation of surveillance cameras in the Data Center. It is anticipated that there will be 24/7 coverage by security guards.

Auditor Recommendation #2:

Install a fire extinguishing system in the Data Center.

Agency Response:

A fire extinguishing system has been installed throughout the Department's new location at 280 Broadway, including the Data Center.

Auditor Recommendation #3:

Install an emergency cut-off switch to shut down power in the event of an emergency.

Agency Response:

The Department does have an emergency cut-off switch. A distribution panel is assigned to the Data Center. In the event of an emergency, the Department shuts down each component of its Data Center systematically, whether there is electricity or not. We do have UPS units that keep Data Center equipment running for 30 to 45 minutes. Sufficient time the Department thinks, before manually tripping the branch circuit breaker and the master switch. At 280 Broadway, the Department will make one change from its procedure at 60 Hudson Street, concerning its emergency cut-off switch. One UPS unit with the capacity to keep the equipment running for 23 minutes will control all the Department's components.

Auditor Recommendation #4:

Install a backup generator at the Data Center.

Agency Response:

There is interrupted power supply at the Department's present location, 60 Hudson Street. At 280 Broadway the Department will have uninterrupted power, supplied from the street. Since there is significant issues surrounding the purchase of a backup generator, the Department is currently analyzing the feasibility of this. Senior managers will meet to discuss purchasing a backup generator at the Data Center.

Auditor Recommendation #5:

Install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system.

Agency Response:

The Department agrees with this recommendation and has started implementing it throughout the Department.

Auditor Recommendation #6:

Have its Personnel Department immediately advise IT of those employees leaving or terminated from the agency. IT should then promptly delete these accounts.

Agency Response:

The Department agrees with this recommendation and is in the process of establishing written procedures regarding deleting accounts for those employees leaving or terminated from the agency. In addition, the Department's Personnel Unit will be required to advise the IT Unit regarding employees separation dates.

Auditor Recommendation #7:

Identity and terminate inactive user accounts.

Agency Response:

In addition to the Agency Response (#6) above, it is the Department current policy of disabling a password after 30 days of inactive use and removing expired passwords after 90 days of inactive use. The Department is making every effort to ensure that the IT unit is following its policy.

Auditor Recommendation #8:

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

Agency Response:

DOB agrees with this recommendation and is currently working with DoITT to establish written procedures regarding DOB mainframe access violations.

Auditor Recommendation #9:

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

Agency Response:

DOB agrees with this recommendation and is currently working to establish formal procedures to document and report network access violations. The Department will also review and follow-up on all reported access violations.

Auditor Recommendation #10:

Ensure that changes to user accounts are made in accordance with its Computing and Networking Policy and Procedures. In this regard, DOB should document when changes to user accounts are requested and approved.

Agency Response:

The agency agrees with the above recommendation and the IT Unit will take additional steps to ensure that any change to users account are documented as indicated in the agency Computing and Networking Policy and Procedures.

Auditor Recommendation #11:

Establish written policies to ensure that only appropriate, authorized changes are made to its application and system software. In this regard, IT officials should document the requests received and the changes IT makes in response to the requests.

Agency Response:

The agency's IT Unit is in the process of establishing written policies to alleviate unauthorized changes to the Department's application and system software. In addition the IT Unit will take additional steps to ensure that changes to users account are documented.

Auditor Recommendation #12:

Complete and formally approve its Network Disaster Recovery Plan. Once the plan is completed and approved, DOB should periodically test it and document the test 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 will devote additional resources to the completion of its Network Disaster Recovery Plan. Once completed the Department will ensure compliance.

Auditor Recommendation #13:

Secure an alternative-processing site for resuming computer operations in the event of a disaster.

Agency Response:

The Department is in the process of installing new network equipment and servers at its new location at 280 Broadway. DOB plans to use the existing network equipment at its present location (60 Hudson Street) and set up an alternative-processing site, most likely in one of our borough offices, in the event of an emergency. The Department's Senior Managers will meet to discuss the location of an emergency site or other viable alternatives.