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 Buildings Data Center

7F05-134

April 7, 2006

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 performed a follow-up audit of the Department of Buildings Data Center.

We audit City facilities such as this to ensure that technological resources critical to the operations of City government are secure, properly updated, maintained, and tested.

The results of our audit, which are presented in this report, have been discussed with officials of the Department of Buildings, and their comments have been considered in preparing this report. Their complete written response are attached to this report.

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

Very truly yours,

William C. Thompson Jr

William C. Thompson, Jr.

WCT/fh

Report: **7F05-134**
Filed: **April 7, 2006**

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

Follow-Up Audit Report on the Department of Buildings Data Center

7F05-134

AUDIT REPORT IN BRIEF

This follow-up audit determined whether the Department of Buildings (DOB) implemented the 13 recommendations made in a previous audit entitled *Audit Report of the Department of Buildings Data Center* (Audit No.7A02-062, issued April 2, 2002). In this report, we discuss the 13 recommendations from the prior audit in detail, as well as the implementation status of each recommendation.

The earlier audit reviewed the adequacy of the Data Center's physical and system security and also determined whether computer operations and contingency plans were adequate and tested in accordance with Comptroller's Directive #18 (Directive #18) and the Federal Information Processing Standards (FIPS). That audit found a number of weaknesses including the following: the Data Center was not monitored on a 24-hour basis, smoke detectors and a fire extinguishing system had not been installed, and the Data Center was not adequately protected from a loss of power. Moreover, DOB had not installed an automated time-out feature on its network; it had not disabled the log-in access of inactive employees; and it had not established formal procedures for documenting, reviewing, and following up on network security violations. Finally, DOB did not have a complete, approved, and tested disaster recovery plan.

Audit Findings and Conclusions

Of 13 recommendations made in the previous audit, this audit disclosed that DOB implemented four, partially implemented four, and did not implement five recommendations. The issues that have not been addressed include: lack of surveillance cameras or a security alarm at the Data Center; lack of backup generator specifically for the Data Center; failure to deactivate user IDs of employees who are no longer working for the agency; lack of procedures developed with the Department of Information Technology & Telecommunications (DoITT) for documenting and reporting mainframe access violations and failed log-in attempts; and non-completion of the alternative-processing site.

Audit Recommendations

To address the issues that still exist, we make the following recommendations, some of which we made in our earlier report. DOB should:

- Install surveillance cameras or a security alarm in the Data Center to monitor the facility on a 24-hour, 7-day-a-week basis.
- Install a backup generator specifically for the Data Center.
- Install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system.
- Ensure that the IT Unit promptly deletes the accounts of terminated employees
- Promptly delete inactive and disabled user IDs.
- Establish formal procedures with DoITT to document and report mainframe access violations, and review and follow up on all reported access violations.
- Establish formal procedures to document and report network access violations and review and follow up on all reported violations.
- Periodically test the disaster recovery plan and document the test results to ensure that it functions as intended.
- Complete the alternative-processing site at its Queens Borough office.

INTRODUCTION

Background

The Department of Buildings oversees building construction and alteration in New York City (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, electric installations, 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 and the Internet, which enables 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.

Within DOB, the Information Technology (IT) department is responsible for developing and supporting application software and for operating the Data Center. The Data Center is the primary DOB data processing facility. The Data Center supports a vast computer network infrastructure that enables DOB to communicate with its remote sites throughout the City.

Objective

This follow-up audit determined whether DOB implemented the 13 recommendations contained in a previous audit, *Audit Report of the Department of Buildings Data Center* (Audit No.7A02-062, issued April 2, 2002).

Scope and Methodology

We reviewed the implementation status of the prior recommendations during the period June 2005 to September 2005. To determine the implementation status of the recommendations, we:

- reviewed the prior audit report issued by the Comptroller's Office, *Audit Report of the Department of Buildings Data Center* (Audit No.7A02-062, issued April 2, 2002);

- toured the Data Center to ascertain whether DOB implemented the physical and system security measures recommended in the previous audit;

- reviewed DOB backup tapes stored at the Staten Island Borough office;

- reviewed DOB’s disaster recovery plan;
- reviewed the DOB *Computer and Networking Policy and Procedure*s;
- compared the DOB user list, dated July 28, 2005, to the New York City Payroll Management System to check whether access to the network has been disabled for employees no longer working for the agency.

As audit criteria we used: Comptroller’s Internal Control and Accountability Directive #18, “Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems”, issued June 29, 1998; the Department of Investigation (DOI) *Citywide Information Security Architecture, Formulation, and Enforcement Policies, Directives, and Standards,* issued April 2003; and the Federal Information Processing 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 City Comptroller’s audit responsibilities 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 DOB officials during and at the conclusion of this audit. A preliminary draft report was sent to DOB officials and discussed at an exit conference held on February 9, 2006. On February 14, 2006, we submitted a draft report to DOB officials with a request for comments. We received a written response from the Department on February 27, 2006. The Department generally agreed with our recommendations and indicated that it is currently in the process of implementing them. The full text of the Department’s response is included as an addendum to this report.

RESULTS OF FOLLOW-UP AUDIT

Of 13 recommendations made in the previous audit, this audit disclosed that DOB implemented four, partially implemented four, and did not implement five recommendations. The issues that have not been addressed include: lack of surveillance cameras or a security alarm at the Data Center; lack of a backup generator specifically for the Data Center; failure to deactivate user IDs of employees who are no longer working for the agency; lack of procedures developed with DoITT for documenting and reporting mainframe access violations and failed log-in attempts; and non-completion of the alternative-processing site.

Please note that the redactions of text in the following sections are the locations associated with the Department's Data Center.

Previous Finding: **"**DOB has not installed a security system to monitor the Data Center continuously."

Previous Recommendation #1: DOB officials should "install surveillance cameras or an alarm system in the Data Center to monitor the facility on a 24 hour, 7-day a week basis."

Previous DOB Response: "The Department is in the process of relocating to [redacted] 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."

Current Status: PARTIALLY IMPLEMENTED

DOB has installed surveillance cameras in the Data Center; however, these cameras are not monitored on 24-hour, 7-day-a-week basis by security guards. Therefore, we consider recommendation #1 partially implemented.

Previous Finding: "Although the Data Center has portable fire extinguishers, it is not equipped with smoke detectors and a fire extinguishing system."

Previous Recommendation #2: DOB officials should "install a fire extinguishing system in the Data Center."

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

Current Status: IMPLEMENTED

Although DOB has not equipped the Data Center with smoke alarms to fully comply with the provisions of Directive #18, the Data Center is now equipped with a fire extinguishing system including an alarm system, an emergency electrical cutoff switch, and sprinklers. Therefore, we consider recommendation # 2 implemented.

<u>Previous Finding</u>: "DOB . . . has not installed an emergency cut-off switch . . . at the Data Center."

Previous Recommendation #3: DOB officials should "install an emergency cut-off switch to shut down power in the event of an emergency."

Previous 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 [uninterrupted power system] 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 [redacted], the Department will make one change from its procedure at [redacted], 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."

<u>Current Status</u>: IMPLEMENTED

We verified that DOB installed an emergency cut off switch in the Data Center that can be used to shut down Data Center power in the event of an emergency. Accordingly, we consider recommendation #3 implemented.

<u>Previous Finding</u>: "DOB . . . has not installed . . . a backup power generator at the Data Center."

Previous Recommendation #4: DOB officials should "install a backup generator at the Data Center."

Previous DOB Response: "There is interrupted power supply at the Department's present location, [redacted]. At [redacted] 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."

<u>Current Status</u>: NOT IMPLEMENTED

DOB did not install a backup generator for its Data Center when it moved to its [redacted] location. In addition, although DOB stated that its senior managers would meet to discuss this issue, it did not provide us with evidence that such meetings actually took place. Therefore, we consider recommendation #4 not implemented.

Previous Finding: "DOB's network is not equipped with a time-out feature that automatically locks workstations after extended periods of inactivity."

Previous Recommendation #5: DOB officials should "install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system."

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

Current Status: NOT IMPLEMENTED

DOB's network still does not have a time-out function to lock workstations after periods of extended inactivity. Therefore, we consider recommendation #5 not implemented.

Previous Finding: **"**Inactive and former employees' log-in access are not actively controlled."

Previous Recommendation #6: DOB officials should "have its Personnel Department immediately advise IT of those employees leaving or terminated from the agency. IT should then promptly delete these accounts."

Previous 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."

Current Status: PARTIALLY IMPLEMENTED

DOB provided written procedures, DOB's *Computing and Network Policy and Procedures*, and evidence that the agency's Personnel Unit informed the IT Unit of employees' separation dates; however, we found that 11 former employees (these employees had been separated from the agency for more than 30 days) still had active network user Ids. Therefore, we consider recommendation #6 partially implemented.

Previous Recommendation #7: DOB officials should **"**identify and terminate inactive user accounts."

Previous DOB Response: "In addition to the Agency Response (#6) above, it is the Department current policy [namely] 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."

Current Status: NOT IMPLEMENTED

We discovered 693 disabled accounts that had not been permanently deleted from DOB's computer environment. Also, 571 employee user accounts had not logged into the system for more than 90 days, thereby violating DOI's "User Account Management Directive," which states, "The system software or operating system must provide for disabling of user IDs after thirty (30) days of inactivity and allow for reactivation with formal approval when necessary. After six (6) months of inactivity, user accounts must be purged from City agency systems." Therefore, we consider recommendation #7, not implemented.

Previous Finding: "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."

Previous Recommendation #8: DOB officials should **"**establish formal procedures with DoITT to document and report mainframe access violations, and review and follow up on all reported access violations."

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

Current Status: PARTIALLY IMPLEMENTED

DoITT informs the agency of security violations by providing DOB with RACF (Resource Access Control Facility) reports, which document mainframe access violations, when requested. However, DOB has not established formal procedures with DoITT to review and follow up on all reported access violations. Accordingly, we consider recommendation #8 partially implemented.

Previous Finding: "DOB does not have procedures to ensure that security violations on its network are recorded, documented, and reviewed."

Previous Recommendation #9: DOB officials should "establish formal procedures to document and report network access violations and review and follow-up on all reported access violations."

Previous 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."

Current Status: NOT IMPLEMENTED

Although DOB provided an "error log" of network access activity, there are no formal procedures to document and report network access violations and review and follow up on all reported access violations. Therefore, we consider recommendation #9 not implemented.

Previous Finding: "DOB does not document when new accounts or changes to user accounts are requested and approved."

Previous Recommendation #10: DOB officials should "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."

Previous 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."

Current Status: IMPLEMENTED

DOB now maintains such documentation and provided it to us; the documentation indicates when new accounts or changes to user accounts are requested and approved. Accordingly, we consider recommendation #10 implemented.

Previous Finding: "DOB does not document when changes to application and system software are requested and approved."

Previous Recommendation #11: DOB officials should "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."

Previous 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."

Current Status: IMPLEMENTED

DOB provided written policies that require recording program changes for applications and system software and for records changes on a form entitled "Infrastructure Upgrade Detailed Checklist." Accordingly, we consider recommendation #11 implemented.

Previous Finding: “DOB has no complete, formally approved, and periodically tested disaster recovery plan.”

Previous Recommendation #12: DOB officials should “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.”
Previous DOB Response: “The Department will devote additional resources to the completion of its Network Disaster Recovery Plan. Once completed the Department will ensure compliance.”

Current Status: PARTIALLY IMPLEMENTED

DOB provided an approved disaster recovery plan. However, although the plan was successfully implemented during the August 2003 blackout, it has not been periodically tested. Accordingly, we consider recommendation #12 partially implemented.

Previous Finding: DOB has no alternative-processing site to bring the system up and running in the event of emergencies or system failure.”

Previous Recommendation #13: DOB officials should “secure an alternative-processing site for resuming computer operations in the event of a disaster.”

Previous DOB Response: “The Department is in the process of installing new network equipment and servers at its new location at [redacted]. DOB plans to use the existing network equipment at its present location ([redacted]) 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.”

Current Status: NOT IMPLEMENTED

Although its disaster recovery plan indicates that DOB intends to use its Queens Borough office as its alternative-processing site, DOB has not installed any of the necessary equipment to complete the process. Therefore, we consider recommendation #13 not implemented.

RECOMMENDATIONS

To address the issues that still exist, some of which we made in our earlier report, we make the following recommendations. DOB should:

1. Ensure that the Data Center is monitored on a 24-hour, 7-day-a-week basis.

***Department Response*: "**We agree, and this recommendation has been partially implemented. The building at [redacted]s guarded and controlled 24/7. In addition, access to both doors to the 6th floor area that houses the Data Center has controlled access by swipe card and only for selected staff. We presently have an environmental sensor unit that also has a functioning camera so that network staff and facilities staff can observe the inside of the network room. We are also planning an upgrade to the swipe card system so that the system is integrated and entrances can be recorded and the data later retrieved for analysis. The current keypad system on the Data Center door limits the number of staff who can enter the Data Center; and this keypad system will soon be replaced with the new swipe card system. Access will be extremely limited to the same Network and Management staff who currently have access via the keypad system.

"The Department is in the process of securing funds from OMB to install cameras which will monitor certain areas such as the [redacted] Street entrance and several in the IT area, especially the Data Center and stock room."

2. Install a backup generator specifically for the Data Center.

***Department Response*: "**Although it would be ideal, we cannot agree to this expectation due to the limitations of the landmark building at [redacted]. Since the Department has exhausted options, we consider this recommendation implemented. The current DCAS generator at [redacted] is sized to support only emergency backup power for life support systems. The Department has been provided with emergency power receptacles for key devices in various building locations. Although other critical systems are not connected to the emergency generator, the phone system and main computer room ([redacted]) are equipped with UPS units. The phone system can function during an emergency. The Data Center ([redacted]) has a 50kva UPS unit with 36 battery cabinet; it is designed to maintain power for 92 minutes and allow systems and network administrators to perform emergency shutdown.

"When balancing the cost of installing and maintaining a generator for the Data Center against the cost of restoring applications at Queens, the generator scenario seems to be much too costly even if it were possible. Feedback from DCAS on multiple occasions is that neither installing a large generator nor utilizing the existing generator are viable options. Therefore, the Department recommends that we stay with the UPS solution coupled with the Queens (or DoITT) alternate site concept, rather than the generator approach. Therefore, we consider this recommendation implemented."

***Auditor Comment**:* The Department of Investigation's Directive entitled *"Physical Security"* §3.4.1 Backup Power for Power Outage Situations specifically states; "[the agency's] supporting infrastructure (for example, air-conditioning and security-alarm systems) must have a dependable, consistent electrical power supplies that are free from surges and interference that could negatively affect their operation. . . . Where appropriate, generators and batteries must also be used to ensure the continuation of operations. In areas susceptible to outages of more than 15 to 30 minutes, diesel generators are recommended. Backup power facilities must be tested regularly to ensure reliable functionality." Therefore, we reiterate our recommendation and further recommend that DOB meet with representatives from the Department of Investigation to review DOB's current strategy to ensure that it meets DOI's Directive."

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

***Department Response*:** "We agree, and have implemented this recommendation. The Network staff has recently tested and implemented a time-out feature that will lock the workstation after fifteen (15) minutes as required by the DOI directive. This lock-out feature has been added to the workstation operating system image so that new computers will be built with this feature. For existing workstations, the feature has been distributed via Track-IT Deploy."

4. Ensure that the IT Unit promptly deletes the accounts of terminated employees.

   ***Department Response*:** "We agree, and have implemented this recommendation."

5. Promptly delete inactive and disabled user IDs.

   ***Department Response*:** "We agree, and have implemented this recommendation."

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

Department Response: "We agree, and this recommendation has been partially implemented. The Department's mainframe application is BIS and BIS ID management is handled through a combination of DoITT and the DOB Security Administrator. For mainframe access violations, we currently receive a daily email of all access violations, and our security administrator reviews it to see if there are any violations that look 'out of the ordinary.' He follows up on critical violations by contacting the user or Borough Manager. We contacted DoITT, and they do not have 'formal procedures' with any other agency, therefore we have sent the . . . process to them for their review and consideration.

“DOB and DoITT are working together to ensure this process satisfies the needs to protect data investments. However, as discussed in the Exit Conference, **all** BIS data is public information. We will continue to ensure, though, that the DOI guidelines are instituted for BIS IDs.”

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

Department Response**:** “We agree, and this recommendation has been partially implemented. For network access violations, the IT unit has recently completed a proof of concept for software and hardware (MAZU) which will record and document network security violations.”

8. Periodically test the disaster recovery plan and document the test results to ensure that it functions as intended.

Department Response**:** “We agree, and have implemented this recommendation.”

9. Complete the alternative-processing site at its Queens Borough office.

Department Response**:** “While we agree with this recommendation and have begun the necessary planning and testing, it has not yet been implemented. . . . We are developing the detailed infrastructure requirements and the detailed task plan now. We hope to be able to test in Queens by April 2006.”

NYC BUILDINGS

NYC Department of Buildings
280 Broadway, New York, NY 10007

Patricia J. Lancaster, FAIA, Commissioner

Marilyn King Festa
Deputy Commissioner
Information Technology
212.566.4225
212.566.3075 fax
marilynk@buildings.nyc.gov

February 27, 2006

Mr. Greg Brooks
Deputy Comptroller
Policy, Audits, Accountancy & Contracts
The City of New York
Office of the Comptroller
1 Centre Street
New York, N.Y. 10007

RE: Follow-Up Audit Report on the Department of Buildings Data Center 7F05-134

Dear Mr. Brooks:

We appreciate this opportunity to respond to the above-mentioned draft report, which is a follow-up audit to determine whether the Department of Buildings implemented the thirteen (13) recommendations made in the previous Audit Report of the Department of Buildings Data Center (Audit No.7A02-062, issued April 2, 2002). In this report, the thirteen (13) recommendations from the prior audit are discussed in detail as well as the implementation status of each.

Following are clarifying comments and our responses to the report's nine (9) recommendations along with references to points that were addressed during the audit process and during the Exit Conference.

Clarifying Comments

We feel it is important to preface the recommendations with comments intended to further clarify the purpose and operations of our 280 Broadway Data Center which is the focus of this audit. We feel it is important to address two (2) statements made on page three (3), third (3rd) paragraph, of the report to avoid any misunderstandings about the Department of Building's computing environment.

First, the statement "The Data Center is the primary DOB data processing facility." should be clarified. Actually BIS is **the** critical application and it runs on DoITT's platforms. Our primary dependence is on DoITT's hosting facilities for BIS and the public's access to information, BISWeb.

Second, the statement "The Data Center supports a vast computer network infrastructure that enables DOB to communicate with its remote sites throughout the City." also needs clarification. Actually our remote sites connect **directly** to DoITT's wide area network through their own independent fiber connections to CityNet. As such, they can access both BIS and BISWeb **without** the 280 Data Center altogether. The statement implies that borough offices connect directly to 280 Data Center which they do not.

Responses to Recommendations

Recommendation 1: ***The Data Center should be monitored on a 24-hour, 7 days-a-week basis.***

Response: We agree, and this recommendation has been partially implemented.

The building at 280 Broadway is guarded and controlled 24/7. In addition, access to both doors to the 6th floor area that houses the Data Center has controlled access by swipe card and only for selected staff.

We presently have an environmental sensor unit that also has a functioning camera so that network staff and facilities staff can observe the inside of the network room.

We are also planning an upgrade to the swipe card system so that the system is integrated and entrances can be recorded and the data later retrieved for analysis. The current keypad system on the Data Center door limits the number of staff who can enter the Data Center; and this keypad system will soon be replaced with the new swipe card system. Access will be extremely limited to the same Network and Management staff who currently have access via the keypad system.

The Department is in the process of securing funds from OMB to install cameras which will monitor certain areas such as the Reade Street entrance and several in the IT area, especially the Data Center and stock room. However, it should be noted that there is an exposure here to potential litigation on several counts - one of which may be the expectation of staff that a camera implies safety 24/7. These cameras would be used primarily as a monitoring device for *after the fact* forensics. To utilize them for real-time monitoring would entail additional resources and even then, safety would not be assured.

Recommendation 2: ***Install a back-up generator specifically for the Data Center.***

Response: Although it would be ideal, we cannot agree to this expectation due to the limitations of the landmark building at 280 Broadway. Since the Department has exhausted options, we consider this recommendation implemented.

The current DCAS generator at 280 Broadway is sized to support only emergency backup power for life support systems. The Department has been provided with emergency power receptacles for key devices in various building locations. Although other critical systems are not connected to the emergency generator, the phone system and main computer room (Room 640) are equipped with UPS units. The phone system can function during an emergency. The Data Center (Room 640) has a 50kva UPS unit with 36 battery cabinet; it is designed to maintain power for 92 minutes and allow systems and network administrators to perform emergency shutdown.

In June of 2004, DOB requested that DCAS install an emergency generator in 280 Broadway to support this agency's Emergency Command Center. DCAS indicated that the structure of the building was such that it could not sustain the weight load of a generator with the capacity that DOB needed even if it was placed in the basement. DOB Facilities and IT staff approached the DCAS resident engineer for 280 Broadway again in the summer of 2005 and requested that the Data Center be added to the existing generator. We were told that the generator is of limited capacity (basically to support emergency lighting) and could not accommodate the electrical load that the Data Center requires.

The Department understands that a graceful shutdown of the Data Center equipment is not the same thing as having a fully functioning Data Center backed up by a generator. However, keeping the Data Center going without HVAC presents the problem of overheating equipment. Essential staff from 280 would still have to go to Queens or other borough offices to work. The current Disaster Recovery plan calls for IT department relocating to Queens and restore only selected applications at Queens: shared files from 280, PIPES and the Intranet.

When balancing the cost of installing and maintaining a generator for the Data Center against the cost of restoring applications at Queens, the generator scenario seems to be much too costly even if it were possible. Feedback from DCAS on multiple occasions is that neither installing a large generator nor utilizing the existing generator are viable options. Therefore, the Department recommends that we stay with the UPS solution coupled with the Queens (or DoITT) alternate site concept, rather than the generator approach. Therefore, we consider this recommendation implemented.

Recommendation 3: ***Install an automatic time-out function on its network to lock workstations after a specified period of inactivity on the system.***

Response: We agree, and have implemented this recommendation.

The Network staff has recently tested and implemented a time-out feature that will lock the workstation after fifteen (15) minutes as required by the DOI directive. This lock-out feature has been added to the workstation operating system image so that new computers will be built with this feature. For existing workstations, the feature has been distributed via Track-IT Deploy.

This implementation now allows a longer application timeout based upon discussions with DOI over workstation lockout versus application controlled timeouts. DOI has agreed that when the workstation lockout feature is installed, BIS and other "green screen" applications can have increased application controlled lockout times.

Therefore, given the implementation of the workstation time-out feature, DOB considers this recommendation implemented.

Recommendation 4: ***Ensure that the IT Unit promptly deletes the accounts of terminated employees.***

Response: We agree, and have implemented this recommendation.

DOB has implemented the following Terminated Employees' Standard Operating Procedure (SOP):

1.Human Resources (HR) staff sends an email to the Help Desk supervisor with the names of users that have been terminated and whose Exit Conferences have been completed.

2.A Help Desk Work Order is created with the following information: Name of Employee, Name of Work Unit, last Date of employee's employment, and the HR staff who sent the email to the Help Desk.

3.A Work Order confirmation is sent back to the HR staff.

4.The Work Order is assigned to the Network Administrator.

5.The terminated employee's Novell ID and Outlook email ID are immediately disabled.

6.The terminated employee's network drive folder is moved to a special "terminated employee" folder on the network with extremely limited access rights.

7.The terminated employee's archived email file(s) is moved to the "terminated employee" folder.

8.The terminated employee's active email is archived to the "terminated employee" folder.

9.The terminated employee's workstation local hard drive is examined for non-system files created by the employee and those files are copied to the "terminated employee" folder.

10. If the terminated employee has been designated on a special WTC data preservation list, the terminated employee's workstation local hard drive is removed, cataloged and preserved in the LAN room.

11. Once all data and emails relating to that employee have been preserved in the "terminated employees" folder, the Work Order is updated as to this status and closed.

Recommendation 5: ***Promptly delete inactive and disabled user IDs.***

Response: We agree, and have implemented this recommendation.

A disabled account can be indicative of an extended absence, a terminated employee, an employee not logging into the network for an extended period, or the employee inadvertently revoking his/ her password. Please note that disabling an account prevents **any** access to the Network and data on that ID.

Nonetheless, DOB has implemented the following Disabled and Inactive IDs Standard Operating Procedure (SOP).

1.A Network Administration monitors these accounts on a weekly basis.

2.The Network Administrator contacts the employee's supervisor to confirm employment status.

3.If the employee has been terminated, then the

"Terminated Employee SOP" is invoked.

4.If disabled only due to an extended absence, then a note is made of this and the account stays in disabled status until the employee returns to work in the expected timeframe. HR sends an email when an employee returns to work after an extended absence. Often the account is periodically activated by the employee's supervisor for special data retrieval. Once that data is retrieved, the account is then disabled again.

5.If disabled only due to lack of use, the Network Administrator resets the account with a new password and contacts the employee to ensure that the employee uses the account and changes the password. (These instances will be reduced drastically since the new Department policy is that all users must have an email account and **must** log on to their email from their desktop at least once per week.)

6.If disabled only due to a revoked password, the employee's password is reset and the employee is notified. (Generally the employee contacts the Help Desk immediately upon this occurrence.)

Recommendation 6: ***Establish formal procedures with DoITT to document and report mainframe access violations, and review and follow-up on all reported violations.***

Response: We agree, and this recommendation has been partially implemented.

The Department's mainframe application is BIS and BIS ID management is handled through a combination of DoITT and the DOB Security Administrator.

For mainframe access violations, we currently receive a daily email of all access violations, and our security administrator reviews it to see if there are any violations that look"out of the ordinary". He follows up on critical violations by contacting the user or Borough Manager. We contacted DoITT, and they do not have "formal procedures" with any other agency, therefore we have sent the following process to them for their review and consideration:

Security Incident Reporting

1.DoITT will automatically send a daily email of all Access violations to DOB's Security Administrator (DOB SA).

2.DOB Security Administrator will maintain a record of all Incident Reports.

Security Incident Analysis

3.DOB Security Administrator will review daily all violations to look for patterns and/or trends.

Security Incident Management

4.DOB Security Administrator will contact authorized user to validate/and verify if there indeed was an attempt by unauthorized users to gain access to their mainframe account.

5.DOB Security Administrator will take appropriate action, such as ID revocation, and notify DOI/ IAD/ DOB IT Management if a suspected or actual/ attempted breach has occurred.

DOB and DoITT are working together to ensure this process satisfies the needs to protect data investments. However, as discussed in the Exit Conference, **all** BIS data is public information. We will continue to ensure, though, that the DOI guidelines are instituted for BIS IDs.

Recommendation 7: ***Establish formal procedures to document and report network access violations and review and follow-up on all reported violations.***

Response: We agree, and this recommendation has been partially implemented.

For network access violations, the IT unit has recently completed a proof of concept for software and hardware (MAZU) which will record and document network security violations. It includes threshold alerts and notifications as well as historical trend analysis. We are in the process of obtaining funding to purchase it. We should have the requested funding by the end of March 2006 and can then purchase the device and fully implement the network violation monitoring, filtering, alerting, and reporting solution.

Recommendation 8: ***Periodically test the disaster recovery plan and document the test results to ensure it functions as intended.***

Response: We agree, and have implemented this recommendation.

As explained to the auditors during the audit process and again during the Exit Conference, BIS is our primary application and it is hosted **completely** at DoITT. None of it is hosted in the 280 Data Center. Even our primary communication with the public, BISWeb is completely hosted at DoITT. Together, these two applications are considered the essential database and processing systems that must be in place for the Department to have the critical level of business continuity in an emergency.

We participate in DoITT's periodic DR testing, which has always been successful. All of our sites can access BIS and BISWeb even if the 280 Data Center is **totally** out of commission. Therefore, it is only our internal smaller applications hosted at 280 that need to be rebuilt in Queens in order to have **full** business continuity. Depending upon the scope and duration of a disaster, this may or may not be a chosen action. Our CORE business, hosted at DoITT, can take place without the 280 Data Center.

The Department's current Disaster Recovery plan assumes that the alternative processing site for our smaller, departmental applications, will be our Queens borough office. However, since approval and release, DoITT has offered to also host a 24/7 DR site for the Department. This is an attractive alternative since DoITT has also recently completed work to make FISA a DR site for the DoITT hosts. If we use DoITT rather than Queens, then we have two levels of DR capability. The discussions will begin in earnest during the first quarter of calendar year 2006.

In addition, the Department began discussions in late 2005 with IBM, who has won the Citywide emergency business recovery contract whereby during large-scale disasters, IBM can procure hardware, software and physical space to ensure business continuity of mission critical processing. We are in planning with DoITT and IBM to determine how best to utilize this service. We also plan to use this service for assessing completeness and testing of the Department's Disaster Recovery plan.

The DOB Disaster Recovery plan has recently been updated to include the business continuity process that was invoked during the transit strike. This updated version was provided to the auditors during the Exit Conference.

Overall our CORE business can take place without the 280 Data Center. Therefore, we consider this recommendation implemented.

Recommendation 9: ***Complete the alternative-processing site at its Queens Borough office.***

Response: While we agree with this recommendation and have begun the necessary planning and testing, it has not yet been implemented.

As explained to the auditors during the audit and again during the Exit Conference, BIS is our primary application and it is hosted

completely at DoITT. None of it is hosted in the 280 Data Center. Even our primary communication with the public, BISWeb is completely hosted at DoITT. Together, these two applications are considered the essential database and processing systems that must be in place for the Department to have the critical level of business continuity in an emergency.

All of our sites can access BIS and BISWeb even if the 280 Data Center is totally out of commission. Therefore, it is only our internal smaller applications hosted at 280 that need to be rebuilt in Queens in order to have **full** business continuity. Depending upon the scope and duration of a disaster, this may or may not be a chosen action. Our CORE business can take place without the 280 Data Center.

For full capability to be restored, we will continue planning and testing the Queens alternative site scenario. We are developing the detailed infrastructure requirements and the detailed task plan now. We hope to be able to test in Queens by April 2006.

Thank you once again for giving us the opportunity to respond to the draft report. We look forward to receiving your final version.

Yours truly,

Marilyn King-Festa

Marilyn King-Festa
Deputy Commissioner of Technology and Analysis

cc: Patricia J. Lancaster, FAIA
Fred D'Alo
Matti Friedman
Walter Bristol
Richard Bernard
Peggy Willens
Katheryne McMullen