AUDIT REPORT

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

Audit Report on the New York City Police Department Data Center

7A06-093

August 14, 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 audited the New York City Police Department's (NYPD) data center.

The data center provides data-processing operations for the NYPD Local Area Networks (LAN) and mainframe computers. The data center also maintains and supports more than 35 computer applications. We audit such City data centers to ensure that they have adequate physical and computer system security controls to prevent unauthorized access.

The results of our audit, which are presented in this report, have been discussed with NYPD officials, and their comments have been considered in preparing this report. Their complete written response is 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: **7A06-093**
Filed: **August 14, 2006**

Table of Contents

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

Audit Report on the New York City Police Department Data Center

7A06-093

AUDIT REPORT IN BRIEF

This office performed an audit on the New York City Police Department (NYPD) data center. The Management Information Systems Division (MISD) is responsible for the data center computer operations that provide information to the entire NYPD. The data center provides data-processing operations for the NYPD Local Area Networks (LAN) and mainframe computers. The data center also maintains and supports more than 35 computer applications. MISD is responsible for implementing and periodically testing the disaster-recovery plan of the data center.

Audit Findings and Conclusions

NYPD has adequate physical security controls that allow only authorized MISD staff members and other approved NYPD personnel access to the data center. MISD also monitors data-center activities 24 hours a day, 7 days a week, as required. NYPD has system security policies and procedures in place. In addition, it has a formalized disaster recovery plan, and this plan is periodically tested. NYPD has also hired an outside vendor to provide an alternate processing site and disaster-recovery services in the event of an operational disaster at or affecting the data center.

However, there are four control weaknesses that should be addressed. Specifically, some inactive user accounts have not been disabled or deleted; the uninterruptible power supply (UPS) lasts only 12 minutes, which may not be a sufficient amount of time for the backup generators to be turned on in the event of a disaster; backup tapes, while stored off-site, are not properly secured in a restricted access area of the premises; and the Department of Investigation (DOI) has not reviewed or approved the NYPD Internet plan, as required.

Audit Recommendations

To address these issues, we recommend that NYPD:

- Ensure that it is following its policy and procedure for reviewing and terminating inactive users and users who have left City service.

- Adhere to DOI policies, directives, and standards, and contact DOI to review and approve its Internet security plan and ascertain that the controls in place are effective.

- Establish and implement procedures to document the Internet activities, the traffic passing through the firewalls, and the penetration-test results.

- Increase the time that the UPS units operate to provide additional time for manual activation of the backup generators in the event of an emergency.

- Store backup tapes in a restricted and secure area.

INTRODUCTION

Background

The New York City Police Department (NYPD) protects lives and property by responding to emergency calls, investigating crimes, and apprehending violators. The department also responds to disasters; keeps order at public events, demonstrations, and civil disturbances; intervenes in family disputes; refers people in distress to appropriate social-service agencies; hires, trains, and supervises City school safety agents; and works in partnership with communities to achieve crime prevention. NYPD relies on its extensive computer systems to keep track of many types of data associated with its mission and to assist its personnel in carrying out their responsibilities.

The Management Information Systems Division (MISD) is responsible for the data center computer operations that provide information to the entire NYPD. MISD plans and coordinates the implementation of advanced technology in support of NYPD programs and initiatives through NYPD support staff and contracts with vendors. The data center provides data-processing operations for the NYPD Local Area Networks (LAN) and mainframe computers 24 hours a day, 7 days a week. The data center also maintains and supports more than 35 computer applications, such as its Automated Roll Call System, On-Line Booking System, On-Line Compliant System, and Live Scan Fingerprinting System. MISD is responsible for implementing and periodically testing of the disaster-recovery plan of the data center. NYPD has contracted with an outside vendor to provide an alternative processing site and disaster-recovery services in order to resume data-processing operations in the event of a disaster at the data center.

Objectives

The audit's objectives were to determine whether the NYPD has adequate:

- physical and computer-system security in its data center;

- Computer operations and contingency plans that have been tested in compliance with applicable Federal Information Processing Standards (FIPS) and City guidelines.

Scope and Methodology

Our audit fieldwork was conducted from October 2005 through April 2006. To achieve our audit objectives, we:

- interviewed NYPD personnel;

- toured the data center and examined its physical security to ascertain whether the NYPD complied with the applicable FIPS and City guidelines;

- reviewed, analyzed, and tested NYPD's compliance with its own operating policies and procedures;

- reviewed and analyzed computer-system security controls to determine whether NYPD complied with applicable New York City Department of Investigation (DOI) policies and directives;

- reviewed, analyzed, and tested whether NYPD had password controls and procedures that were adequate and complied with the DOI's Information Security Directive;

- reviewed NYPD's *Information Security Policy Overview*;

- reviewed and analyzed NYPD's user list, dated December 17, 2005, to determine whether employees no longer working for the agency had access to its computer environment;

- reviewed and analyzed NYPD user-aging reports produced through its mainframe, dated January 12, 2006, and through its network, dated January 19, 2006, to determine whether users periodically changed passwords as required and whether the monitoring software performed as intended;

- reviewed, analyzed, and assessed whether the NYPD network and mainframe user profiles complied with DOI Directives;

- reviewed NYPD policies and procedures for storing backup tapes to ascertain whether the physical security for these tapes is adequate;

- sampled 30 back-up tapes from NYPD logs and verified that these tapes were located at the specific site noted;

- reviewed and evaluated whether the NYPD disaster-recovery plan complies with City standards; and

- checked whether the NYPD disaster-recovery plan had been recently tested and that any outstanding issues had been addressed.

As audit criteria, we used: the New York City Comptroller's Internal Control and Accountability Directive #18, "Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems"; the National Institute of Standards and Technology (NIST) Generally Accepted Principles and Practices for Securing Information Technology Systems; the Federal Information Processing Standards (FIPS); and the DOI Citywide Information Security Architecture, Formulation and Enforcement (Information Security Directive.)

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 NYPD officials during and at the conclusion of this audit. A preliminary draft report was sent to NYPD officials and discussed at an exit conference held on May 25, 2006. On June 12, 2006, we submitted a draft report to NYPD officials with a request for comments. We received a written response from NYPD on June 30, 2006. In their response, NYPD agreed with four of the five recommendations made in this audit. The recommendation that NYPD disagreed with relates to increasing the time criteria for the UPS units however NYPD proposes a compensating control that will alert the operators to systemically and safely shut down the system.

The full text of NYPD's comments is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

NYPD has adequate physical security controls that allow only authorized MISD staff members and other approved NYPD personnel access to the data center. MISD also monitors data center activities 24 hours a day, seven days a week, as required. NYPD has system security policies and procedures in place. In addition, NYPD has a formalized disaster-recovery plan, and this plan is periodically tested. It has also hired an outside vendor to provide an alternate processing site and disaster-recovery services in the event of an operational disaster at or affecting the data center.

However, there are four control weaknesses that should be addressed. Specifically: some inactive user accounts have not been disabled or deleted; the uninterruptible power supply (UPS) lasts only 12 minutes, which may not be a sufficient amount of time for the backup generators to be turned on in the event of a disaster; backup tapes, while stored off-site, are not properly secured in a restricted access area of the premises; and DOI has not reviewed or approved NYPD’s Internet plan, as required.

These matters are discussed in the following sections of this report.

Physical Security

Physical security is the most basic and commonly addressed information-processing environment control. It encompasses safeguarding not only computer facilities and general work areas, but also includes areas housing such essential support equipment as air conditioning, communications lines, network and communication hubs, power control panels, and storage of tapes and disks.

NYPD has adequate physical security controls that allow only authorized MISD staff members access to the data center. Other NYPD personnel need authorization from MISD to enter the data center. Further, MISD has installed cameras with which police officers and MISD staff monitor data-center activities 24 hours a day, seven days a week. A card key access-control system at the data center entrance prevents unauthorized access. The data center is also equipped with smoke detectors, fire alarms, separate air conditioning units, and humidity and temperature controls.

Computer System Security

Overall, NYPD has adequate computer-system security controls that include user-account and password policies and procedures. NYPD produces and regularly reviews its system security violation reports. These reports document any instance when system security has been violated, including the time such violation occurred, the user password accountable for the violation, and what resource was accessed. Moreover, the mainframe security software, Resource Access Control Facilities, is designed to prevent unauthorized access to the system.

This software restricts the access of authorized users to only those computer resources, functions, and facilities that are required to perform their jobs.

User Accounts Are Not Adequately Controlled

Although NYPD has adequate computer-system security controls, it has not disabled or deleted some inactive user accounts. MISD provided us a list of current mainframe user accounts as of December 2005. However, we found that many user accounts have an "unknown" status. According to MISD officials, those users with unknown status never logged onto the mainframe system. MISD provided us a user-aging report that showed that 15,241 of 43,000 mainframe user accounts never initially logged onto the system from 1995 to 2005. The aging reports also showed that 1,145 of 14,053 LAN users never initially logged onto the system, and that 1,009 users had not logged onto the system for the previous six months. Comptroller's Directive #18, §8.1.2, states "active password management includes deactivation of inactive user accounts and accounts for employees whose services have terminated." Neglecting to delete inactive user accounts increases the system's vulnerability to inappropriate access and abuse.

Internet Security Not Reviewed By DOI

NYPD has Internet security policies and procedures in place. However, the DOI Citywide Information Security, Architecture, Formulation, and Enforcement (CISAFE) has not reviewed or approved the NYPD Internet plan. As prescribed in DOI Directive §2.3, "Information Security Risk Assessment," which states "Implementation of security controls is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE." The responsibilities of CISAFE include enforcement of the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems. Therefore, it is imperative that the NYPD Internet plan be reviewed to ensure that it has appropriate controls.

A vital goal of the City is to ensure that all its computer systems are adequately protected against information security vulnerabilities. In that regard, the fact that DOI CISAFE has not reviewed NYPD Internet plan is of concern. DOI CISAFE proactively develops and disseminates security solutions, security policies, directives, and standards to ensure the integrity of system security. The implementation of security controls is the responsibility of each City agency over the systems it uses and maintains. However, DOI is mandated to monitor the effectiveness of agency system-security controls to ensure integrity. Without documentation that the controls cited by NYPD over its internet security were implemented or of a thorough review and approval by DOI, the NYPD computer environment may be vulnerable to unauthorized access and abuse.

Internet Security Controls Not Documented

Further, NYPD officials stated that the agency has installed security filtering software to restrict access by NYPD personnel to unauthorized Internet sites. NYPD also installed firewalls to monitor and restrict Internet activities, and conducts penetration testing on its data-processing environment to minimize the risk of unauthorized access from non-NYPD personnel. However, NYPD provided no proof that those controls exist or that they have been tested. Without the proper controls the NYPD's computer environment may be vulnerable to unauthorized access and abuse.

Recommendation

NYPD MISD should:

1. Ensure that it is following its policy and procedure for reviewing and terminating inactive users and users that have left City service.

   NYPD Response: **"**NYPD/MISD has already implemented a process to delete dormant users from our system. This process will run periodically in order to identify additional dormant accounts."

2. Adhere to DOI policies, directives, and standards and contact DOI to review and approve its Internet security plan and ascertain that the controls in place are effective.

   NYPD Response: "The NYPD's Internet plan is in the draft stages and is pending final approval prior to forwarding to the Department of Investigation. Firewall penetration testing will be documented in accordance with the recommendation with a sufficient amount of detail for future review."

3. Establish and implement procedures to document the Internet activities, the traffic passing through the firewalls, and the penetration-test results.

   NYPD Response: "Firewall penetration testing will be documented appropriately and with a sufficient amount of detail for future review."

<u>Computer Operations</u>

The term "computer operations" includes the day-to-day operation and maintenance of all computer resources, including hardware, software, networks, and telecommunications. This also includes providing the technical and support processes necessary to run a computer in its intended environment and to perform its intended functions.

NYPD computer operations are adequately maintained. NYPD has formal program-change control procedures to document changes on the system, system maintenance reporting, system problem-management reporting, and equipment-problem reporting. These reports are maintained and reviewed on a regular basis by management. In addition, NYPD maintains an inventory of its hardware and software, including the license agreements from the manufacturer of the software installed in its computers, and equipment. It has contracted with an outside vendor, IBM, to provide hardware maintenance, software licenses, and software maintenance for all IBM mainframe products. These contracts were duly registered with the Comptroller's Office.

NYPD has installed an emergency cut-off switch, three backup power generators, and two UPS units. These provide electric power to the data center prior the activation of the backup generator. In the event of an emergency, the UPS units should also provide sufficient time to shut down critical computer operations without damage or loss of data. However, together the two UPS units can keep the NYPD's data center running for only 12 minutes. NYPD representatives stated that this is sufficient time for the backup generators to automatically activate. So, any unforeseen event that prevents the activation of these generators within the 12-minute interval, thereby forcing NYPD personnel to manually start these generators, would shut down NYPD operations, and expose the City to considerable risk.

Recommendation

4. NYPD should increase the time that the UPS units operate to provide additional time for manual activation of the backup generators in the event of an emergency.

   NYPD Response: "The current UPS system is designed to provide adequate battery power at full load. At the present time, the current load provides double the standard of normal battery life. Once the system has detected an external power outage, the generators located within 1 Police Plaza will automatically start within seconds. In addition, the generators can be manually started in the event that there is some unforeseen problem. The manufacturer of the UPS was contacted and stated that our battery runtime per system is more than adequate.

   "To enhance the response of an unforeseen power outage, the plant management unit will have an audible/visual alarm installed within the data-center. The system will consistently monitor the UPS batteries and sound an alarm when it detects that the batteries are under a load. An additional alarm will be activated if the generators fail to engage allowing ample time to systematically bring the system down."

   Auditor Comment: Although, NYPD disagreed with the recommendation, it proposed a compensating control to install an audible/visual alarm within the data center that will alert the operators that the batteries are below load. However, NYPD should provide the operators adequate time to shut down computer operations without material loss of data in the event that manual activation of the backup generators incur any unforeseen emergency.

<u>Disaster Recovery Plan</u>

NYPD has a formal disaster-recovery plan in place, which was tested on March 5, 2006. The plan identified the steps to be followed to restore computer operations in the event of an emergency or disaster. MISD provided us the results of this Citywide test and a schedule indicating how often and when testing of the plan would be performed. NYPD also has contracted with an outside vendor to provide an alternative processing site and disaster-recovery services to resume data-processing operations in the event of a disaster. The contract will provide disaster services within 24 hours after NYPD has declared the disaster. The contract covers the period extending from January 2004 to December 2008, and was properly registered with the Comptroller's Office. We reviewed documentation and logs that substantiate that there is a point-to-point daily backup at the data center and simultaneously at the backup site. These logs also indicate that MISD also performs weekly and monthly backup activities at the data center.

Storage of Backup Tapes

We observed that backup tapes are stored both at the NYPD premises and off-site. Our walk-through of the off-site premises revealed that backup tapes are stored in locked cabinets in the public hallway. Comptroller's Directive #18, §7.0, states, "Physical controls constitute the first level of defense in the protection of the information processing environment. Protection from vandalism, theft . . . are all elements of physical security." This unsecured storage area leaves the tapes susceptible to theft or destruction by an unforeseen event. In this regard, storing the tapes in the public hallway exposes the entire disaster-recovery and contingency plan to significant risk, due to the potential loss of mission critical data.

Recommendation

5. NYPD should store backup tapes in a restricted and secure area.

   NYPD Response: "Back-up tapes are currently stored in a locked cabinet within a secure NYPD facility. To ensure total security, all tapes will be moved to another location in one of the five boros that has 24 hour, 7 day a week police security. The location is alarmed and is currently being prepared for tape storage. The tapes will be secured in a locked room accessible only to NYPD/MISD personnel. This move will be completed in approximately six weeks."

The City of New York

POLICE DEPARTMENT
Office of Management Analysis and Planning
One Police Plaza, Room 1403
New York, N.Y. 10038

June 23, 2006

Mr. John Graham
Deputy Comptroller, Audits Accountancy and Contracts
The City of New York Office of the Comptroller
Executive Offices
1 Centre Street
New York, N.Y. 10007-2341

Re: Draft Report of the Audit of the NYPD Data Center (Audit # 7A06-093)

Dear Mr. Graham:

We wish to thank the Comptroller for the opportunity to review this draft report of the audit on the Police Department's Data Center and comment on the auditor's findings and recommendations. We trust that our comments on the draft will be seriously considered by your office and reflected in the audit's final report.

It is gratifying that the Comptroller found that the NYPD has adequate physical security controls that allow only authorized MISD staff and other approved NYPD personnel access to the Data Center. It is also pleasing to know that the Comptroller found that the NYPD has adequate computer system controls and procedures in place, has a formalized disaster recovery plan which is periodically tested, and uses an outside vendor to provide an alternate processing site in the event of an operational disaster affecting the Data Center.

We agree with your recommendations that the NYPD should ensure that it is following its policy and procedures for reviewing and terminating inactive users, and that it should adhere to the Department of Investigation's policies, directives, and standards. We also agree that the Department should establish and implement procedures to document internet activities in addition to storing back up tapes in a restricted and secure area.

Attached, as per your request, please find an Audit Implementation Plan indicating the Department's response to each of the Comptroller's recommendations. The Department agrees with recommendation #'s 1, 2, 3, and 5, but disagrees with recommendation #4. For security reasons many of the exact specifications regarding time criteria for the UPS units to operate or the storage locations of backup tapes have not been indicated on the response form.

In addition to safeguards that have already been built into the present system to ensure that the Data Center is continuously active, the Department intends to install an automatic audio/visual alarm which will activate when the UPS batteries are under a system load. An additional alarm will be installed which will activate if the generators fail to engage after a predetermined amount of time.

We appreciate the Comptroller's efforts in conducting this review of the Data Center and hope that your office found that the Department has continued to demonstrate its policy of cooperation during the course of the audit. If you have any questions concerning this response, please call Administrative Staff Analyst Kenneth Wesley at 646-610-8366.

Sincerely,

John P. Gerrish
Deputy Chief
Commanding Officer
Office of Management
Analysis and Planning

NYPD AUDIT IMPLEMENTATION PLAN

Auditing Agency	NYC Comptroller
Audit Title/Subject	NYPD/MISD Data Center Audit
Audit #	7A06-093

AUDIT REPORT STATUS	Draft Report	Report Dated	6/12/2006

PD EVALUATION OF RECOMMENDATIONS BY CATEGORY

Category		Recommendation Numbers	Total Recommendations
A	We agree with the recommendation and have implemented or will attempt to implement	1,2,3,5	4
B	We agree with the recommendation but are unable to implement		
C	We disagree with the recommendation and will not implement.	4	1
D	The recommendation, while valid, is unnecessary because it calls for an action, policy or practice that was planned or existed independent of the audit.		
E	We must further analyze/evaluate the recommendation.		
TOTAL – All Recommendations Made			5

LIST OF RECOMMENDATIONS AND PD EVALUATION OF EACH

#	Recommendation	Category				
		“A” Agree. Will Imple-Ment.	“B” Agree. Can't Imple-Ment.	“C” Disagree. Won't Imple-Ment.	“D” Not Necessary. A Planned or Existing Practice.	“E” Requires Study.
1.	NYPD should ensure that it is following its policy and procedure for reviewing and terminating inactive users that have left City service.	X				
2.	NYPD should adhere to D.O.I.'s policies, directives, and standards and contact D.O.I. to review and approve its internet security plan and ascertain that the controls in place are effective.	X				
3.	NYPD should establish and implement procedures to document the Internet activities, the traffic passing through the firewalls, and the penetration results.	X				
4.	NYPD should increase the time that the UPS units operate to provide additional time for manual activation of the backup generators in the event of an emergency.			X		
5.	NYPD should store backup tapes in a restricted and secure area.	X				

Category "A"	We agree with the recommendation and have implemented or will attempt to implement.

Recommendation #	1.		Report Page #	8
Recommendation				
NYPD should ensure that it is following its policy and procedure for reviewing and terminating inactive users that have left City service.				
Implementation Methods/Procedures and Projected/Actual Implementation Date				
NYPD/MISD has already implemented a process to delete dormant users from our system. This process will run periodically in order to identify additional dormant accounts.				

Recommendation #	2.		Report Page #	8
Recommendation				
NYPD should adhere to D.O.I.'s policies, directives, and standards and contact D.O.I. to review and approve its internet security plan and ascertain that the controls in place are effective				
Implementation Methods/Procedures and Projected/Actual Implementation Date				
The NYPD's Internet plan is in the draft stages and is pending final approval prior to forwarding to the Department of Investigation. Firewall penetration testing will be documented in accordance with the recommendation with a sufficient amount of detail for future review.				

Recommendation #	3.		Report Page #	8
Recommendation				
NYPD should establish and implement procedures to document the Internet activities, the traffic passing through the firewalls, and the penetration results.				
Implementation Methods/Procedures and Projected/Actual Implementation Date				
Firewall penetration testing will be documented appropriately and with a sufficient amount of detail for future review.				

Recommendation #	5.		Report Page #	9
Recommendation				
NYPD should store backup tapes in a restricted and secure area.				
Implementation Methods/Procedures and Projected/Actual Implementation Date				
Back-up tapes are currently stored in a locked cabinet within a secure NYPD facility. To ensure total security, all tapes will be moved to another location in one of the five boros that has 24 hour, 7 day a week police security. The location is alarmed and is currently being prepared for tape storage. The tapes will be secured in a locked room accessible only to NYPD/MISD personnel. This move will be completed in approximately six weeks.				

Category "C"	We disagree with the recommendation and will not implement.

Recommendation #	4		Report Page #	9
Recommendation				
NYPD should increase the time that the UPS units operate to provide additional time for manual activation of the backup generators in the event of an emergency.				
Explanation				
The current UPS system is designed to provide adequate battery power at full load. At the present time, the current load provides double the standard of normal battery life. Once the system has detected an external power outage, the generators located within 1 Police Plaza will automatically start within seconds. In addition, the generators can be manually started in the event that there is some unforeseen problem. The manufacturer of the UPS was contacted and stated that our battery runtime per system is more than adequate. To enhance the response of an unforeseen power outage, the plant management unit will have an audible/visual alarm installed within the data-center. The system will consistently monitor the UPS batteries and sound an alarm when it detects that the batteries are under a load. An additional alarm will be activated if the generators fail to engage allowing ample time to systematically bring the system down.				