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
Police Department's
Mainframe Data Center**

7A02-156

June 5, 2002

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

Audit Report on the
Police Department's
Mainframe Data Center

7A02-156

EXECUTIVE SUMMARY

Background

The New York City Police Department's (NYPD) mission is to protect lives, safeguard the property of City residents and visitors, and maintain civil order. NYPD responds to emergencies, disasters, and crime reports; apprehends criminals; processes fire and medical emergency calls; maintains order at public events and demonstrations; enforces car traffic and parking rules; and performs community services in areas of public school safety, general public safety, crime prevention, family disputes, domestic violence, quality of life, and social service agency referrals.

NYPD uses three mainframe computers: A single-processor mainframe computer system supporting the mission-critical Special Police Radio Inquiry Network (SPRINT) computer-assisted dispatching system for response to the public's emergency "911" calls; and a dual-processor mainframe computer system for processing more than 50 other (i.e., non-SPRINT) mission and administrative support applications. NYPD's Management Information System Division (MISD) is responsible for the data center operations, as well as for developing, implementing, and periodically testing the data center's disaster recovery plans.

Objectives

Our audit objectives were to: review the adequacy of the data center's physical security and computer system security, and determine whether computer operations and contingency plans are adequate and have been tested in compliance with applicable federal and City guidelines.

Scope and Methodology

Audit fieldwork began in March 2002 and ended in April 2002. To meet our objectives, we: interviewed agency personnel; toured the data center and examined its physical security; reviewed and analyzed the data center's data security controls; reviewed and analyzed the data center's operating policies; reviewed and evaluated NYPD's Disaster Recovery Plan for SPRINT; reviewed and evaluated NYPD's procurement documentation for a Disaster Recovery Plan covering the non-SPRINT computer operations; and reviewed and tested NYPD compliance with certain federal and City guidelines.

Results in Brief

NYPD has adequate physical security controls, computer system controls, and operational and general controls in place to ensure that the data center is adequately safeguarded. Physical security at the data center is above standard. Data backup is performed and computer operating statistics are regularly reviewed for problems. In addition, detailed system downtime reports are maintained, which allows management to correct systemic problems.

However NYPD does not have formal test procedures for its SPRINT system's Disaster Recovery Plan, and it has not fully implemented a Disaster Recovery Plan for its non-SPRINT computer operations. We made two recommendations, that NYPD officials should:

1. Establish formal testing procedures as part of SPRINT's Disaster Recovery Plan. Specifically, NYPD should:
   - Determine the proper test frequency and establish a test schedule;
   - Develop test objectives and establish individual participant assignments;
   - Document the test results, including notations of any changes to hardware and software configurations; and
   - Implement a formal test result review process to address any open issues.

2. Attempt to expedite the approval process of the contracting for the non-SPRINT disaster recovery services by ensuring that all necessary items for approval are in place. In this regard, NYPD should contact each approval agency to emphasize the importance of this backup system and to determine what information that agency still needs to receive before it approves the contracting.

NYPD Response

The matters covered in this report were discussed with officials from NYPD during and at the conclusion of this audit. A preliminary draft was sent to NYPD

officials and discussed at an exit conference held on May 7, 2002. On May 8, 2002, we submitted a draft report to NYPD officials with a request for comments. We received a written response from NYPD on May 28, 2002. NYPD agreed with the audit's findings and recommendations.

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

Table of Contents

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

Audit Report on the
Police Department's
Mainframe Data Center

7A02-156

INTRODUCTION

Background

The New York City Police Department's (NYPD) mission is to protect lives, safeguard the property of City residents and visitors, and maintain civil order. NYPD responds to emergencies, disasters, and crime reports; apprehends criminals; processes fire and medical emergency calls; maintains order at public events and demonstrations; enforces car traffic and parking rules; and performs community services in areas of public school safety, general public safety, crime prevention, family disputes, domestic violence, quality of life, and social service agency referrals.

NYPD uses three mainframe computers to process data and provide information in support of its mission, as follows:

- A single-processor mainframe computer system that processes mission-critical applications. This system, known as the Special Police Radio Inquiry Network (SPRINT) is a computer-assisted dispatching system that supports NYPD's response to the public's emergency calls to the citywide emergency "911" telephone number.

- Two mainframe computers that process more than 50 other (i.e., non-SPRINT) user applications—for crime information gathering, tracking, and processing—as well as applications for agency administrative support.

NYPD's Management Information System Division (MISD) is responsible for operating and maintaining the mainframe computer data center. MISD is also responsible for developing, implementing, and periodically testing the data center's disaster recovery plans.

Objectives

Our audit objectives were:

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

- To determine whether computer operations and contingency plans are adequate and have been tested in compliance with applicable federal and City guidelines.

Scope and Methodology

Audit fieldwork began in March 2002 and ended in April 2002. To meet our objectives, we:

- Interviewed agency personnel;

- Toured the data center and examined its physical security;

- Reviewed and analyzed the data center's data security controls;

- Reviewed and analyzed the data center's operating policies;

- Reviewed and evaluated NYPD's Disaster Recovery Plan for SPRINT;

- Reviewed and evaluated NYPD's procurement documentation for a Disaster Recovery Plan covering the non-SPRINT computer operations; and

- Reviewed and tested NYPD compliance with federal and City guidelines.

We used as our audit criteria the Federal Information Processing Standards (FIPS), Comptroller's Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems* (Directive 18), and the Department of Investigation's (DOI) Directive, *Information Security Guideline–Business Continuity*, dated February 22, 2002.

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.

NYPD Response

The matters covered in this report were discussed with officials from NYPD during and at the conclusion of this audit. A preliminary draft was sent to NYPD officials and discussed at an exit conference held on May 7, 2002. On May 8, 2002, we submitted a draft report to NYPD officials

with a request for comments. We received a written response from NYPD on May 28, 2002. NYPD agreed with the audit's findings and recommendations.

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

OFFICE OF THE COMPTROLLER
NEW YORK CITY

DATE FILED: June 5, 2002

FINDINGS AND RECOMMENDATIONS

NYPD has adequate physical security controls, computer system controls, and operational and general controls in place to ensure that the data center is adequately safeguarded.   Specifically:

- Physical security at the data center was above standard—no unauthorized individual can gain access to the data center;

- Data backup is performed—daily backup is performed, and backup data is stored offsite;

- Computer operating statistics are regularly reviewed to determine whether system problems exist; and,

- Detailed system downtime reports are maintained, which allows management to correct systemic problems.

However NYPD does not have formal test procedures for its SPRINT system's Disaster Recovery Plan, and it has not fully implemented a Disaster Recovery Plan for its non-SPRINT computer operations.

The SPRINT Disaster Recovery Plan
Lacks Adequate Testing Procedures

NYPD has a Disaster Recovery Plan covering SPRINT operations. The plan provides for data processing backup at another major City data center in the event its data center becomes inoperable. NYPD last tested the SPRINT Disaster Recovery Plan in June 2001. However, NYPD did not provide us with a schedule indicating how often and when testing of the plan would be performed, the test objectives, the responsibilities of individual participants in the tests, the specific items to be tested, and the test result review process.

FIPS 87 states:

> "One of the more important aspects of successful contingency planning is the continual testing and evaluation of the plan itself. Quite simply, a plan which has not been tested cannot be assumed to work. Likewise, a plan documented, tested once and then filed away to await the day of need provides no more than a false sense of security. . . . The devising of test plans which adequately and reliably exercise the contingency plan themselves require considerable skill and great care so as to meet the objective of providing tests which are entirely realistic while still being economically feasible. . . . The test plans should form a formal part of the contingency plan documentation and be as fully subject to the review and approval process as the other sections of the plan."

In addition, DOI's Guidelines state:

"Periodic reviews and updates are necessary to ensure that the BCP [Business Continuity Plan] remains current. A comprehensive test should be conducted at least annually. The test objectives and results must be documented and signed by a responsible BCP representative within the City agency."

The increasing dependence on computers and data processing support makes it critical that NYPD officials regularly test and document its Disaster Recovery Plan.

The Non-SPRINT Disaster Recovery Plan
Is Not Fully Implemented

NYPD has not fully implemented a Disaster Recovery Plan covering all non-SPRINT computer operations. NYPD is in the process of procuring the services of an outside vendor to provide non-SPRINT data processing services in the event of an operational disaster at NYPD's data center. This would effectively provide NYPD with an effective Disaster Recovery Plan. However, NYPD cannot complete the procurement process until approval is received from various City agencies. Until this process is completed, its non-SPRINT systems are not protected against loss due to an unforeseen event.

Recommendations

NYPD officials should:

1. Establish formal testing procedures as part of SPRINT's Disaster Recovery Plan. Specifically, NYPD should:

   - Determine the proper test frequency and establish a test schedule,

   - Develop test objectives and establish individual participant assignments,

   - Document the test results, including notations of any changes to hardware and software configurations, and

   - Implement a formal test result review process to address any open issues.

   NYPD Response: "As you indicated, the Department does have a disaster recovery plan in place for its SPRINT operations. The Police Department's Management Information Systems Division is currently finalizing the development of a formal testing procedure for this plan that will contain the elements specified in the recommendation. In addition, MISD has decided to conduct a test every six months. The next test, scheduled for June 2002, will include specific test objectives and participant assignments; we will document test results. After each test the project leaders will meet with the Systems Programming Section/SPRINT Section Manager and MISD's Technical Director to review and address all aspects of the test."

2. Attempt to expedite the approval process of the contracting for the non-SPRINT disaster recovery services by ensuring that all necessary items for approval are in place. In this regard NYPD should contact each approval agency to emphasize the importance of this backup system and to determine what information that agency still needs to receive before it approves the contracting.

   NYPD Response: "The Department recognizes the importance of having a disaster recovery plan for its non-SPRINT computer operations. That is why it is in the process of contracting with IBM to provide such a plan. The Agency's Chief Contracting Officer is attempting to expedite the approval process for this contract by anticipating and providing all of the information needed by the contract approval oversight agencies. At the present time he is working with IBM and the City's Law Department to address any issues. The approvals of the Mayor's Office of Contracts and the Comptroller's Office must also be obtained. These approvals are expected to take about two months."

POLICE DEPARTMENT

Office of Management Analysis and Planning
One Police Plaza, Room 1403

May 28, 2002

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

                                        Re: Mainframe Data Center
                                        Draft Report
                                        [Audit # 7A02-156]

Dear Mr. Liwer:

            The following is the Department's response to the above
report. We welcomed the opportunity to review this draft report and
comment upon the audit's findings and recommendations. Furthermore,
we wish to thank the Comptroller for providing an extension to reply to
the report.

            It is gratifying that the Comptroller found that the "NYPD
has adequate physical security controls, computer system controls, and
operational and general controls in place to ensure that the data center
is adequately safeguarded."

            In addition to the important finding stated above, the report
contains two recommendations. We agree to implement both.

                    Recommendation # 1:_Establish formal testing procedures as_
                                        part of SPRINT's Disaster Recovery
                                        Plan.

                    As you indicated, the Department does have a disaster
                    recovery plan in place for its SPRINT operations. The Police
                    Department's Management Information Systems Division is
                    currently finalizing the development of a formal testing
                    procedure for this plan that will contain the elements
                    specified in the recommendation. In addition, MISD has

decided to conduct a test every six months. The next test, scheduled for June 2002, will include specific test objectives and participant assignments; we will document test results.

After each test the project leaders will meet with the Systems Programming Section/SPRINT Section Manager and MISD's Technical Director to review and address all aspects of the test.

Recommendation #2: *Attempt to expedite the approval process of the contracting for the non-SPRINT disaster recovery services by ensuring that all necessary items for approval are in place.*

The Department recognizes the importance of having a disaster recovery plan for its non-SPRINT computer operations. That is why it is in the process of contracting with IBM to provide such a plan. The Agency's Chief Contracting Officer is attempting to expedite the approval process for this contract by anticipating and providing all of the information needed by the contract approval oversight agencies. At the present time he is working with IBM and the City's Law Department to address any issues. The approvals of the Mayor's Office of Contracts and the Comptroller's Office must also be obtained. These approval are expected to take about two months.

We appreciate the Comptroller's efforts to conduct the audit and prepare the report. We hope your office found that the Department demonstrated its policy of cooperation with the Comptroller's office during the course of the audit.

If you have any questions concerning this response, please call Deputy Audit Coordinator Michael Manzolillo at 646-610-8365.

Sincerely,

Joanne Jaffe
Assistant Chief
Commanding Officer

Copy: M. Manzolillo
       Mayor's Office of Operations

8