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

WILLIAM C. THOMPSON, JR.
Comptroller

Follow-up Audit Report on the Department of Citywide Administrative Services Office of Management Information Systems Implementation of the Agency-Wide Local Area Network

7F02-167

June 20, 2002

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

Follow-up Audit Report on the Department of Citywide Administrative Services Office of Management Information Systems Implementation of the Agency-Wide Local Area Network

7F02-167

SUMMARY OF FINDINGS AND CONCLUSIONS

This follow-up audit determined whether the New York City Department of Citywide Administrative Services' (DCAS) Office of Management Information Systems (OMIS) implemented the recommendations made in a previous audit entitled, *Audit Report of the Department of General Services Office of Management Information Systems Implementation of Agency-Wide Local Area Network* (Audit #7A96-124, issued April 29, 1996). The earlier audit evaluated the implementation phase of the agency-wide Local Area Network (LAN). In our current audit, we discuss the recommendations we made earlier, as well as the implementation status of those recommendations.

In our previous audit we made ten recommendations to DCAS (formerly known as the Department of General Services), of which six have been implemented, one has been partially implemented, two have not been implemented, and one recommendation is no longer applicable. The details of these recommendations and their implementation status follow. DCAS should:

1. "Review and comply with all Citywide regulations describing the development of cost-benefit analysis for new projects, thereby eliminating the need to add or to re-design computer projects. While DGS/OMIS has almost completed the implementation of their LAN, collating any existing cost justification data would assist DGS in future LAN modifications."
   NO LONGER APPLICABLE

2. "Secure the LAN room and the enclosed compartment with the following:
   - Alarms for smoke and fire.
   - A reinforced door to the LAN room.

- A changeable combination lock with an intercom and buzz-in feature.
- An off-hour motion detection and door break-through intruder alarm preferably wired to the first floor lobby and guard's desk.

In addition, we recommend that DGS/OMIS management comply with DOISSS #502, 'Secured Areas'; DOISSS #515, 'Recommendations for the Physical Protection of the Computer Personnel and Installations'; and DOISSS #516, 'Smoke Detectors.'" **IMPLEMENTED**

3. "Develop a comprehensive program for funding, scheduling, and implementing training programs. This program should cover computer usage and safeguards by maximizing the value and improving security of this multi-million dollar LAN investment." **IMPLEMENTED**

4. "Implement a staffing contingency plan to alleviate possible funding limitations for existing per diem staff." **IMPLEMENTED**

5. "Explore cross-training possibilities for existing full-time technical personnel to off-set any potential future displacement of staff (full-time and per diem) in OMIS." **IMPLEMENTED**

6. "Evaluate continued deployment of per diem staff in context of DOISSS #051 and on a cost-versus-benefit basis as opposed to recruiting full-time staff." **IMPLEMENTED**

7. "Develop a plan for a more stable staffing arrangement to more fully meet the tasks of maintaining a multi-million dollar 1,400 user LAN." **IMPLEMENTED**

8. "The Comptroller recommends that OMIS establish formal documentation for the following:
   - Maintenance records (unscheduled system downtime, debugging and periodic maintenance). ***Not Implemented***
   - LAN configuration (workstation and peripheral equipment connection diagrams with communications gateways detail)." ***Implemented***

   Overall Status: **PARTIALLY IMPLEMENTED**

9. "Develop, approve, and implement a Disaster Recovery/Contingency Plan in accordance with Comptroller's Directive #18 and the Department of Investigation's System Security Standards. This plan should include procedures for handling system emergencies, which could occur when the facility is unstaffed." **NOT IMPLEMENTED**

10. "Test such a Disaster Recovery/Contingency Plan to ensure that it will provide smooth, rapid, and effective restoration of the LAN sites' functions in the event of a disaster. We further recommend that any test of such a Disaster

Recovery/Contingency Plan not be announced so that the staff learn how to function during a real emergency." **NOT IMPLEMENTED**

To address the issues that still exist, we now recommend that DCAS management should:

1. Establish formal documentation that records unanticipated downtime and downtime for system debugging and periodic maintenance.

2. Develop, approve, and implement a Disaster Recovery Plan in accordance with Comptroller's Directive 18.

3. Test the Disaster Recovery Plan to ensure that it will provide smooth, rapid, and effective restoration of the LAN sites' functions in the event of a disaster. Any test of such a Disaster Recovery Plan should not be announced so that the staff learn how to function during an actual emergency.

A new issue, Internet connectivity, was raised during the course of this audit. As part of the Department of Investigation (DOI) System Security Standards, agencies that plan to provide agency-wide Internet access must submit a proposal to DOI for approval. According to records we obtained from DOI, DCAS's *Internet Security Plan and Inventory* has been approved.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the City Comptroller's audit responsibilities as set forth in Chapter 5, § 93, of the New York City Charter.

Agency Response

The matters covered in this report were discussed with officials from DCAS during and at the conclusion of this audit. A preliminary draft was sent to DCAS and discussed at an exit conference on May 30, 2002. We submitted a draft report to DCAS on May 30, 2002, with a request for comments. We received a written response on June 13, 2002. DCAS agreed with our recommendations to establish formal documentation for unanticipated downtime and for downtime for system debugging and periodic maintenance, and develop, approve and implement a Disaster Recovery Plan in accordance with Directive 18. DCAS partially agreed with our recommendation to test the Disaster Recovery Plan, stating that a substantial increase in server capacity would be required to test a full LAN restoration. Nevertheless, DCAS stated that it will test sever restorations to the extent of its ability.

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

INTRODUCTION

Background

DCAS, formerly known as the Department of General Services, provides a variety of personnel and administrative support services to City agencies and serves as the City's central procurement agency. DCAS also provides municipal maintenance and supply services for City-owned buildings. In addition, DCAS manages the City's portfolio of leased properties, and manages and oversees energy conservation programs. It runs the City Publishing Center, which publishers the *City Record*, the Green Book, and other official City publications.

DCAS's Office of Management Information Systems (OMIS) is primarily responsible for providing automated information technology services to the agency and for supporting the hardware and software that comprise the DCAS LAN. The DCAS LAN connects user workstations throughout the agency and is the agency's communication gateway from its divisions to the Citynet and to Financial Information Services Agency (FISA) applications. The previous audit focused on the implementation phase of the agency-wide LAN.

Objective, Scope, and Methodology

This follow-up audit determined whether the ten recommendations contained in a previous audit, *Audit Report of the General Services Office of Management Information Systems Implementation of Agency-Wide Local Area Network* (Audit #7A96-124, issued April 29, 1996), were implemented.

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

- toured the LAN computer room;
- reviewed and analyzed DCAS's Disaster Recovery Plan;
- reviewed documentation provided in response to our previous recommendations;
- reviewed Internet security policy and procedures; and
- tested DCAS compliance with Comptroller's Directive 18.

We used as the audit's criterion Comptroller's Internal Control and Accountability Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems* (Directive 18), issued June 29, 1998.

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 also performed in accordance with the City

Comptroller's audit responsibilities as set forth in Chapter 5, § 93, of the New York City Charter.

Agency Response

The matters covered in this report were discussed with officials from DCAS during and at the conclusion of this audit. A preliminary draft was sent to DCAS and discussed at an exit conference on May 30, 2002. We submitted a draft report to DCAS on May 30, 2002, with a request for comments. We received a written response on June 13, 2002. DCAS agreed with our recommendations to establish formal documentation for unanticipated downtime and for downtime for system debugging and periodic maintenance, and develop, approve and implement a Disaster Recovery Plan in accordance with Directive 18. DCAS partially agreed with our recommendation to test the Disaster Recovery Plan, stating that a substantial increase in server capacity would be required to test a full LAN restoration. Nevertheless, DCAS stated that it will test sever restorations to the extent of its ability.

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

OFFICE OF THE COMPTROLLER
NEW YORK CITY

DATE FILED: June 20, 2002

RESULTS OF THIS FOLLOW-UP AUDIT

PREVIOUS FINDING: "Lack of cost-benefit analysis prior to implementation."

> ***Previous Recommendation #1:*** "Review and comply with all Citywide regulations describing the development of cost-benefit analysis for new projects, thereby eliminating the need to add or to re-design computer projects. While DGS/OMIS has almost completed the implementation of their LAN, collating any existing cost justification data would assist DGS in future LAN modifications."
>
> ***Previous Agency Response:*** "The current OMIS Director believes that a cost-benefit analysis report was done by the prior MIS staff. However, when this administration assumed control, all records relating to the implementation of the LAN were misplaced and phase I of the LAN implementation plan was underway. As a result, we have been unable to locate the cost-benefit analysis report and a second was not performed."

Current Status: NO LONGER APPLICABLE

The LAN was fully implemented in 1996. Therefore, the cost-benefit analysis is no longer an issue. Accordingly, we consider Recommendation #1 no longer applicable.

* * * * * *

PREVIOUS FINDING: "OMIS has not developed formal physical security guidelines for the LAN site."

> ***Previous Recommendation #2:*** "Secure the LAN room and the enclosed compartment [that contains the LAN equipment] with the following:
>
> - Alarms for smoke and fire.
> - A reinforced door to the LAN room.
> - A changeable combination lock with an intercom and buzz-in feature.
> - An off-hour motion detection and door break-through intruder alarm preferably wired to the first floor lobby and guard's desk.
>
> In addition, we recommend that DGS/OMIS management comply with DOISSS #502, 'Secured Areas'; DOISSS #515, 'Recommendations for the Physical Protection of the Computer Personnel and Installations'; and DOISSS #516, 'Smoke Detectors.'"
>
> ***Previous Agency Response:*** "While we are aware that the LAN site's physical security needs to be upgraded, we have had to prioritize the use of scarce monies. To address this important issue, we will recommend hiring an expert consultant in physical security to review all recommendations for increased security and the corresponding costs. We will also investigate the use of the current ASR [Agency Service Request] process to determine the needs of the computer room in both security and fire detection."

Current Status: IMPLEMENTED

OMIS has secured the LAN room and the enclosed compartment that contains the LAN equipment with smoke and fire alarms. Further, the main entrance to the LAN room has an intercom, motion detectors, and a cardkey access system. The cardkey access system is connected to both the OMIS Assistant Commissioner's office and the central building security unit. OMIS has also installed a reinforced door that has a changeable combination lock and key to protect the enclosed compartment. Additionally, OMIS is currently installing a surveillance camera that will allow the security unit to monitor LAN room activity. Accordingly, we consider Recommendation #2 implemented.

* * * * * *

PREVIOUS FINDING: "LAN training for users is inadequate."

> ***Previous Recommendation #3:*** "Develop a comprehensive program for funding, scheduling, and implementing training programs. This program should cover computer usage and safeguards by maximizing the value and improving security of this multi-million dollar LAN investment."
>
> ***Previous Agency Response:*** "DGS is in the process of developing an education recommendation for the entire agency. Simultaneously, a private consultant is conducting a survey of all DGS users as well as Department of Personnel users (in anticipation of the merger later this year). The survey results will provide us with an inventory of all software products and the training requirements to effectively use these products."

Current Status: IMPLEMENTED

DCAS now provides its employees with a comprehensive training program that covers computer use and system security, as recommended. Accordingly, we consider Recommendation #3 implemented.

* * * * * *

PREVIOUS FINDING: "OMIS' dependency upon per diem workers to provide continued operations for the LAN site poses a risk to DGS [DCAS]."

> ***Previous Recommendation #4:*** "Implement a staffing contingency plan to alleviate possible funding limitations for existing per diem staff."
>
> ***Previous Recommendation #5:*** "Explore cross-training possibilities for existing full-time technical personnel to off-set any potential future displacement of staff (full-time and per diem) in OMIS."

Previous Recommendation #6: "Evaluate continued deployment of per diem staff in context of DOISSS #051 and on a cost-versus-benefit basis as opposed to recruiting full-time staff."

Previous Recommendation #7: "Develop a plan for a more stable staffing arrangement to more fully meet the tasks of maintaining a multi-million dollar 1,400 user LAN."

Previous Agency Response to #4, #5, #6, and #7: "As of this response, OMIS only has 1 remaining per-diem worker and this contract will expire on June 30, 1996. DGS has used per-diem employees to train staff in troubleshooting and minor system repair. Moreover, the DGS helpdesk has reduced the number of per-diem workers from four to one. We anticipate that all helpdesk staff will be city employees by July of this year."

Current Status to #4, #5, #6, and #7: IMPLEMENTED

OMIS is no longer using per diem employees to operate the LAN. OMIS has increased its staff from 19 to 35 full-time employees for LAN administration, help desk, and application development. OMIS is also in the process of hiring three additional full-time employees for its LAN operations. Accordingly, we consider Recommendations #4, #5, #6, and #7 implemented.

* * * * * *

PREVIOUS FINDING: "Inadequate documentation for some LAN administrative functions."

Previous Recommendation #8: "Establish formal documentation for the following:

- Maintenance records (unscheduled system downtime, debugging and periodic maintenance). ***Not Implemented***
- LAN configuration (workstation and peripheral equipment connection diagrams with communications gateways detail)." ***Implemented***

Previous Agency Response: "We now require all administrative systems staff keep a problem and system log. The log records all scheduled and unscheduled down time. This requirement should allow us to review trends in downtime. We currently contract with NOVELL to periodically review the network to ascertain if it is running at peak performance. The last review of the LAN, done in March of this year received an excellent rating. The Novell engineer informed us that all systems were at peak efficiency and all software patches were up to date."

Current Status: PARTIALLY IMPLEMENTED

OMIS now maintains documentation for its LAN configuration. Specifically, OMIS has an Internet security design and Ethernet wiring diagram that show the connections between hubs, switches, routers, and servers. However, OMIS still does not maintain records of system

downtime, system debugging, and periodic maintenance performed on the LAN. Accordingly, we consider Recommendation #8 partially implemented.

* * * * * *

PREVIOUS FINDING: "OMIS does not have a formally approved Disaster Recovery Plan for the LAN."

> ***Previous Recommendation #9:*** "Develop, approve, and implement a Disaster Recovery/Contingency Plan in accordance with Comptroller's Directive 18 and the Department of Investigation's System Security Standards. This plan should include procedures for handling system emergencies, which could occur when the facility is unstaffed."
>
> ***Previous Recommendation #10*:** "Test such a Disaster Recovery/Contingency Plan to ensure that it will provide smooth, rapid, and effective restoration of the LAN sites' functions in the event of a disaster. We further recommend that any test of such a Disaster Recovery/Contingency Plan not be announced so that the staff learn how to function during a real emergency."
>
> ***Previous Agency Response to #9 and #10:*** "A true disaster recovery system entails the use of a registered HOT site configured to your exact LAN specifications. The DGS does not have nor does it plan to have such an expensive alternative for its LAN. DGS maintains copies of all System and Data files at an offsite facility. All user computers are configured to automatically run as standalone machines should catastrophes occur. As a result, DGS business would continue as usual, but without the ability to communicate via the LAN using E-Mail or shared files. All users are encouraged to maintain backup files on their local computer drives or diskettes in the event that the Network is incapacitated."

Current Status to #9 and #10*:* NOT IMPLEMENTED

DCAS still does not have a Disaster Recovery Plan for its LAN operations. Accordingly, we consider Recommendations #9 and #10 not implemented.

Recommendations

To address the issues that still exist, we now recommend that DCAS management should:

1. Establish formal documentation that records unanticipated downtime and downtime for system debugging and periodic maintenance.

***Agency Response*:** "We agree."

2. Develop, approve, and implement a Disaster Recovery Plan in accordance with Comptroller's Directive 18.

***Agency Response*:** "We agree. We have briefly discussed our current plan and are reevaluating a number of options for improving the Disaster Recovery Plan. We will ensure that this Plan is in accordance with Directive 18."

3. Test the Disaster Recovery Plan to ensure that it will provide smooth, rapid, and effective restoration of the LAN sites' functions in the event of a disaster. Any test of such a Disaster Recovery Plan should not be announced so that the staff learn how to function during an actual emergency.

***Agency Response*:** "Partial Agreement. Without a very substantial increase in server capacity, we believe that it is impossible to test a full LAN restoration. We will test server restorations to the extent of our ability."

NEW ISSUE

A new issue, Internet connectivity, was raised during the course of this audit. As part of the Department of Investigation (DOI) System Security Standards, agencies that plan to provide agency-wide Internet access must submit a proposal to DOI for approval. According to records we obtained from DOI, DCAS's *Internet Security Plan and Inventory* has been approved.

Department of Citywide Administrative Services

Municipal Building, 17th Floor
One Centre Street
New York, N.Y. 10007
(212) 669-7111 Fax: (212) 669-8992
E-Mail: mhirst@dcas.nyc.gov

Martha K. Hirst
Commissioner

June 13, 2002

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

Re: Follow-up Audit on the Department of Citywide Administrative Services Office of Management Information Systems Implementation of the Agency-wide Local Area (7F02-167)

Dear Mr. Liwer:

We have reviewed the draft audit and offer the following comments.

The report states that the Disaster Recovery Plan in place for the Local Area Network is inadequate. This plan was the result of an evaluation of the Network that found that none of the applications that currently reside on the network servers were deemed to be mission critical. As part of the Year 2000 review, these evaluations were shared with the Comptroller's Office, who concurred in our assessment.

The DCAS LAN Disaster Recovery Plan consists of daily system back-ups to tape, off-site storage of these tapes, and restoration of data from these tapes as required. In agencies with mission critical applications, such procedures might be considered part of regular system operations rather than a Disaster Recovery Plan. Disaster Plans for these agencies normally contain provisions for the establishment of "hot sites" and/or alternative processing and operating locations. While we agree that these alternatives would provide the best options for recovering from disaster, in the past it has been difficult for this Agency to cost-justify them. In light of recent events, however, we are currently re-examining all options for our business continuation plan.

Recommendations:

Recommendation 1: Establish formal documentation that records unanticipated downtime and downtime for system debugging and periodic maintenance.

Response: We agree.

Recommendation 2: Develop, approve, and implement a Disaster Recovery Plan in accordance with Comptroller's Directive 18.

Response: We agree. We have briefly discussed our current plan and are reevaluating a number of options for improving the Disaster Recovery Plan. We will ensure that this Plan is in accordance with Directive 18.

Recommendation 3: Test the Disaster Recovery Plan to ensure that it would provide smooth, rapid, and effective restoration of the LAN's functions in the event of a disaster. Any test of such a Disaster Recovery Plan should not be announced so that the staff learns how to function during an actual emergency.

Response: Partial Agreement. Without a very substantial increase in server capacity, we believe that it is impossible to test a full LAN restoration. We will test server restorations to the extent of our ability.

Thank you for the opportunity to comment on this report.

Very truly yours,

Martha K. Hirst