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 Internal Controls for the Department of Citywide Administrative Services Data Center

7F02-166

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 Internal Controls for the Department of Citywide Administrative Services Data Center

7F02-166

SUMMARY OF FINDINGS AND CONCLUSION

This follow-up audit determined whether the New York City Department of Citywide Administrative Services (DCAS) implemented the recommendations made in an earlier audit report, *Audit Report of the Internal Controls for the New York City Department of General Services's FAMIS Data Center* (Audit #7A96-080, issued June 28, 1996). The earlier audit evaluated the adequacy of the data center's physical security, computer operations, and backup/contingency plans. This follow-up audit discusses the recommendations made in the previous audit as well as the implementation status of those recommendations.

The previous audit made 21 recommendations to DCAS (formerly known as the Department of General Services), of which three have been implemented, four have been partially implemented, and 14 are no longer applicable. The details of these recommendations and their implementation status follow. DCAS should:

1. "Develop formal physical security guidelines/procedures concerning the data center. These guidelines should be reviewed and updated periodically." **NO LONGER APPLICABLE**

2. "Improve the physical security of the data center by maintaining a list of staff members who are authorized to have access to the data center, requiring visitors to sign in at all times, and placing a guard outside the data center during evenings and weekends." **NO LONGER APPLICABLE**

3. "Periodically inspect the data center to ensure its cleanliness and safety." **NO LONGER APPLICABLE**

4. "Develop and formally document system administrator policies, procedures, and guidelines that include security procedures to monitor, report, and review system access security violations. In addition, job descriptions should be developed for the system administrator function." **IMPLEMENTED**

5. "Establish formal written security policies and procedures in accordance with Comptroller's Directive 18, the New York City Department of Investigation's System Security Standards for Electronic Data Processing, and New York City's Data Processing Standards. These policies and procedures should provide for the overall safety of the [DCAS] data center hardware and software." **IMPLEMENTED**

6. "Comply with New York City's Department of Investigation System Security Standard #210, which requires that passwords be changed regularly." **PARTIALLY IMPLEMENTED**

7. "Comply with the 'Open VMS Vax Guide to System Security,' which recommends that the security administrator provide tight volume protection through UIC based protection." **NO LONGER APPLICABLE**

8. "Meet with the all City agencies using FAMIS to discuss ways to improve the system's security, including:

    - developing an algorithm that would hide the passwords from view when the security file is printed, ***Implemented***

    - developing procedures for removing users from the FAMIS, ***Implemented***

    - regularly changing passwords and using access control forms, and ***Partially Implemented***

    - regularly reviewing, updating and monitoring their security file for reasonableness and accuracy." ***Implemented***

    Overall Status: **PARTIALLY IMPLEMENTED**

9. "Develop a formal disaster contingency plan. This plan should be reviewed by [DCAS] for content, and periodically tested. A copy of the plan should be kept on site as well as at an off-site location." **PARTIALLY IMPLEMENTED**

10. "Develop formal disaster recovery procedures in order to restore system operations. These procedures should be tested annually." **PARTIALLY IMPLEMENTED**

11. "Ensure that FAMIS' supporting documentation is stored at an off-site location." **IMPLEMENTED**

12. "Install and test an Uninterrupted Power System at the data center." **NO LONGER APPLICABLE**

13. "Enter into a contract with a government agency or private firm to provide disaster recovery facilities, or establish its own back-up facility for data center operations at an off-site location." **NO LONGER APPLICABLE**

14. "Purchase a locking cabinet to properly secure the tape in the on-site library." **NO LONGER APPLICABLE**

15. "Contact Arcus Data Storage Incorporated and instruct this vendor to begin a regularly scheduled tape pickup." **NO LONGER APPLICABLE**

16. "Provide better record keeping ability for the tape library function by purchasing and using an automated tape library management software package." **NO LONGER APPLICABLE**

17. "Update its master inventory listing, and keep it up to date." **NO LONGER APPLICABLE**

18. "Examine its maintenance contract with DEC [Digital Equipment Corporation] to determine whether preventive maintenance is performed on the DEC/VAX mainframe during visits. If DEC is not performing scheduled preventive maintenance, then [DCAS] should schedule preventive maintenance immediately." **NO LONGER APPLICABLE**

19. "Require data center management to meet with the Senior Stationary Engineer from the Facilities Management and Construction unit to establish a regular preventive maintenance schedule for the large air conditioners." **NO LONGER APPLICABLE**

20. "Maintain records of the air conditioning units' downtime, including explanations." **NO LONGER APPLICABLE**

21. "Retain copies of air conditioners' maintenance logs evidencing work performed. [DCAS] should also periodically analyze and review air conditioning maintenance logs and records." **NO LONGER APPLICABLE**

To address the issues from the previous audit that have not been resolved, we now recommend that DCAS:

1. Require that all system users periodically change their passwords.

2. Test the MCMS [Maintenance Control Management System] disaster recovery plan annually.

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 report was sent to DCAS and discussed at an exit conference held on May 30, 2002. On May 30, 2002, we submitted a draft report to DCAS with a request for comments. We received a written response on June 13, 2002. In response to the audit recommendations, DCAS stated that it will revisit the issue of requiring system users to periodically change their passwords and stated that MCMS will be part of DoITT's annual Disaster Recovery Plan test.

The full text of the DCAS 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 chief 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.

During the previous audit, the primary computer system in the agency's data center was the Fleet Administration Maintenance Information System (FAMIS); this system was replaced in 1999 by the Maintenance Control Management System (MCMS). The MCMS system tracks information on vehicles, and vehicle parts, maintenance, and repairs for nine City agencies, including DCAS. In November 1999, MCMS was transferred to a site managed by the Department of Information Technology and Telecommunications (DoITT). This system is currently on the DoITT IBM mainframe computer; therefore, DoITT is responsible for the maintenance of the hardware and the physical security of the system. DCAS retains responsibilities for the system, such as access control and the periodic testing its disaster recovery plan.

The previous report concluded that DCAS did not have formal physical and system security procedures, its data center security needed improvement, the data center was not periodically cleaned, the disaster contingency plan was inadequate, and DCAS did not have adequate control over its FAMIS inventory.

Objective, Scope, and Methodology

This follow-up audit determined whether the 21 recommendations contained in a previous audit, *Audit Report of the Internal Controls for the New York City Department of General Services's FAMIS Data Center* (Audit # 7A96-080, issued June 28, 1996) were implemented.

Our fieldwork was conducted from April 2002 to May 2002. To achieve our objectives, we:

- interviewed DCAS officials;
- reviewed and analyzed data security controls;
- reviewed and examined DCAS's disaster recovery plan;
- tested DCAS compliance with Comptroller's Directive 18.

We used as criteria for this audit, 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, and the Federal Information Processing Standards (FIPS).

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 report was sent to DCAS and discussed at an exit conference held on May 30, 2002. On May 30, 2002, we submitted a draft report to DCAS with a request for comments. We received a written response on June 13, 2002. In response to the audit recommendations, DCAS stated that it will revisit the issue of requiring system users to periodically change their passwords and stated that MCMS will be part of DoITT's annual Disaster Recovery Plan test.

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

OFFICE OF THE COMPTROLLER
NEW YORK CITY
DATA FILED: JUNE 20, 2002

RESULTS OF THIS FOLLOW-UP AUDIT

PREVIOUS FINDING: "Physical security controls and maintenance controls within the FAMIS data center must be improved."

Previous Recommendation #1: DCAS should "develop formal physical security guidelines/procedures concerning the data center. These guidelines should be reviewed and updated periodically."

Previous Agency Response: "We agree and will develop these procedures within the next six months."

Previous Recommendation #2: DCAS should "improve the physical security of the data center by maintaining a list of staff members who are authorized to have access to the data center, requiring visitors to sign in at all times, and placing a guard outside the data center during evenings and weekends."

Previous Agency Response: "We agree to implement the use of a visitors log, however, it is not possible for [DCAS] to hire a 24-hour, seven-day a week security guard."

Current Status of #1 and #2: NO LONGER APPLICABLE

The system was transferred in November 1999 to a facility managed by DoITT. Therefore, DCAS is no longer responsible for the physical security of the mainframe. Accordingly, we consider Recommendations #1 and #2 no longer applicable.

******

PREVIOUS FINDING: "Facility maintenance should be improved."

Previous Recommendation #3: DCAS should "periodically inspect the data center to ensure its cleanliness and safety."

Previous Agency Response: "We agree and will review the contract with EMS to assure the cleanliness and safety of the data center."

Current Status: NO LONGER APPLICABLE

Since the system is now housed in a DoITT facility, DCAS is no longer responsible for maintaining the system. Accordingly, we consider Recommendation #3 no longer applicable.

******

PREVIOUS FINDING: "System/security administration function [needs to] be improved."

Previous Recommendation #4: DCAS should "develop and formally document system administrator policies, procedures, and guidelines that include security procedures to monitor, report, and review system access security violations. In addition, job descriptions should be developed for the system administrator function."

Previous Agency Response: "We agree and will develop the procedures and job description within the next six months."

Current Status: IMPLEMENTED

DCAS now has formal security procedures for the system. The procedures cover system access and include the responsibilities of the system administrator, as required by Comptroller's Directive 18. Accordingly, we consider Recommendation #4 implemented.

Previous Recommendation #5: DCAS should "establish formal written security policies and procedures in accordance with Comptroller's Directive 18, the New York City Department of Investigation's System Security Standards for Electronic Data Processing, and New York City's Data Processing Standards. These policies and procedures should provide for the overall safety of the [DCAS] data center hardware and software."

Previous Agency Response: "We agree and once we are in receipt of the various standards mentioned formal written procedures will be done."

Current Status: IMPLEMENTED

Since the system is now housed in a DoITT facility, DCAS is no longer responsible for system hardware security. However, DCAS is responsible for software control and has provided us a copy of the software control procedures. Accordingly, we consider Recommendation #5 implemented.

****

PREVIOUS FINDING: "System users' password control procedures are inadequate."

Previous Recommendation #6: DCAS should "comply with New York City's Department of Investigation System Security Standard #210, which requires that passwords be changed regularly."

Previous Agency Response: "As we stated above, this is not [DCAS'] area of responsibility. We will, however, forward to the various FAMIS liaisons a copy of the Department of Investigation's system Security Standard #210."

Current Status: PARTIALLY IMPLEMENTED

MCMS system administrators (DCAS personnel authorized to add, change, and delete users from the system) are required to change their passwords periodically. However, DCAS does not require that users change their passwords. Accordingly, we consider Recommendation #6 partially implemented.

Previous Recommendation #7: DCAS should "comply with the 'Open VMS Vax Guide to System Security,' which recommends that the security administrator provide tight volume protection through UIC based protection."

Previous Agency Response: "We agree and will implement as soon as possible."

Current Status: NO LONGER APPLICABLE

The previous recommendation refers to the Digital Equipment Corporation (DEC) guide to its system security for FAMIS. However, the DEC system is no longer in use since FAMIS has been replaced by MCMS, which has been incorporated into DoITT's IBM mainframe. Accordingly, we consider Recommendation #7 no longer applicable.

Previous Recommendation #8: DCAS should "meet with the all City agencies using FAMIS to discuss ways to improve the system's security, including:

- developing an algorithm that would hide the passwords from view when the security file is printed, ***Implemented***
- developing procedures for removing users from the FAMIS, ***Implemented***
- regularly changing passwords and using access control forms, and ***Partially Implemented***
- regularly reviewing, updating and monitoring their security file for reasonableness and accuracy." ***Implemented***

Previous Agency Response: "We agree and plan to schedule meetings in the near future."

Current Status: PARTIALLY IMPLEMENTED

DCAS provided us a copy of the system security procedures that cover access control. The procedures also include the review and monitoring of security files that hide user passwords from view. However, DCAS does not require other users at other

agencies to regularly change their passwords. Accordingly, we consider Recommendation #8 partially implemented.

******

PREVIOUS FINDING: "Disaster recovery planning is inadequate."

> ***Previous Recommendation #9:*** DCAS should "develop a formal disaster contingency plan. This plan should be reviewed by [DCAS] for content, and periodically tested. A copy of the plan should be kept on site as well as at an off-site location."
>
> ***Previous Recommendation #10:*** DCAS should "develop formal disaster recovery procedures in order to restore system operations. These procedures should be tested annually."
>
> ***Previous Agency Response:*** "As we stated in our response to audit report: 'Audit Report of the Department of General Services Office of Management Information Systems Implementation of Agency-Wide Local Area Network' (#7A96-124, April 29, 1996), a true disaster recovery plan entails the use of a registered HOT site configured to your system's specification. [DCAS] does not have nor does it plan to have such an expensive alternative for FAMIS."

Current Status of #9 and #10: PARTIALLY IMPLEMENTED

DCAS provided a copy of their *MCMS Disaster Recovery Plan*. DCAS officials stated that this plan is also kept at the other eight agencies that use MCMS. However, DCAS did not test the plan annually. DCAS provided documentation showing that the plan was last tested in November 1999. Accordingly, we consider Recommendations #9 and #10 partially implemented.

******

PREVIOUS FINDING: "Critical documentation is not stored off-site."

> ***Previous Recommendation #11:*** DCAS should "ensure that FAMIS' supporting documentation is stored at an off-site location."
>
> ***Previous Agency Response:*** "We agree and at this time, all FAMIS users have documentation on site."

Current Status: IMPLEMENTED

MCMS's supporting documentation, including the disaster recovery plan and the system's user manual, is retained at the other eight agencies that use the system. Accordingly, we consider Recommendation #11 implemented.

******

PREVIOUS FINDING: "No alternative power back-up in the current data center."

Previous Recommendation #12: DCAS should "install and test an Uninterrupted Power System at the data center."

Previous Agency Response: "We agree and, as soon as purchasing approval is granted, we will comply."

Current Status: NO LONGER APPLICABLE

The protection and recovery of mainframe hardware and the data stored on the system are now DoITT's responsibilities. Therefore, we consider Recommendation #12 no longer applicable.

******

PREVIOUS FINDING: "No alternative processing site for FAMIS."

Previous Recommendation #13: DCAS should "enter into a contract with a government agency or private firm to provide disaster recovery facilities, or establish its own back-up facility for data center operations at an off-site location."

Previous Agency Response: "We will explore the possibility of contracting with other government agencies for disaster recovery facilities."

Current Status: NO LONGER APPLICABLE

Since the system is now housed in a DoITT facility, DCAS is no longer responsible for providing an alternative processing site for MCMS. Accordingly, we consider Recommendation #13 no longer applicable.

******

PREVIOUS FINDING: "Tape library management controls need improvement."

Previous Recommendation #14: DCAS should "purchase a locking cabinet for storing tapes in the on-site library."

Previous Agency Response: "[DCAS] has a locking cabinet for storing tapes in the on-site library."

Previous Recommendation #15: DCAS should "contact Arcus Data Storage Incorporated and instruct this vendor to begin a regularly scheduled tape pickup."

Previous Agency Response: "Under a new contract, Arcus Stat Storage Incorporated will now provide monthly pickup of tapes."

Previous Recommendation #16: DCAS should "provide better record keeping ability for the tape library function by purchasing and using an automated tape library management software package."

Previous Agency Response: "We will explore the possibility of purchasing an automated tape library management software package."

Current Status of #14, #15, and #16: NO LONGER APPLICABLE

DoITT is now responsible for storing system back-up tapes. Accordingly, we consider Recommendations #14, #15, and #16 no longer applicable.

******

PREVIOUS FINDING: "[DCAS'] hardware inventory controls need improvement."

Previous Recommendation #17: DCAS should "update its master inventory listing, and keep it up to date."

Previous Agency Response: DCAS disagreed with this recommendation. It stated "a current inventory is available from the OMIS Deputy Director. . . . The current hardware inventory is not kept on FAMIS as it states in the report. Rather, the OMIS Deputy Director (who is responsible for the data center) keeps an updated listing in separate files for the purpose of administering and monitoring all maintenance contracts for FAMIS software and hardware, including that in the field. The Deputy Director was not asked at any time during the audit to confirm that the inventory list was the most current available. Had this information been requested from the appropriate person, in this case the Deputy Director, the auditors would have received the latest inventory list for FAMIS hardware."

Current Status: NO LONGER APPLICABLE

Since the system is now housed in a DoITT facility, DCAS is no longer responsible for the hardware inventory controls for MCMS. Accordingly, we consider Recommendation #17 no longer applicable.

******

PREVIOUS FINDING: "There has been no preventive maintenance performed on the DEC/VAX mainframe."

Previous Recommendation #18: DCAS should "examine its maintenance contract with DEC to determine whether preventive maintenance is performed on the DEC/VAX mainframe during visits. If DEC is not performing scheduled preventive maintenance, then [DCAS] should schedule preventive maintenance immediately."

Previous Agency Response: DCAS disagreed with this recommendation. It stated, "EMS performs the preventive maintenance and DEC performs service calls when a piece of hardware goes down."

Current Status: NO LONGER APPLICABLE

DoITT is responsible for the preventive maintenance of the mainframe. Accordingly, we consider Recommendation #18 no longer applicable.

******

PREVIOUS FINDING: "There are no maintenance logs showing that preventive maintenance is performed on air conditioning units."

Previous Recommendation #19: DCAS should "require data center management to meet with the Senior Stationary Engineer from the Facilities Management and Construction unit to establish a regular preventive maintenance schedule for the large air conditioners."

Previous Recommendation #20: DCAS should "maintain records of the air conditioning units' downtime, including explanations."

Previous Recommendation #21: DCAS should "Retain copies of air conditioners' maintenance logs evidencing work performed. [DCAS] should also periodically analyze and review air conditioning maintenance logs and records."

Previous Agency Response #19, #20, and #21: "We agree and will establish a protocol with the Division of Facilities Management and Construction in the near future."

Current Status of #19, #20 and #21: NO LONGER APPLICABLE

DoITT is responsible for the preventive maintenance of the air conditioning units in its computer facility. Accordingly, we consider Recommendations #19, #20, and #21 no longer applicable.

Recommendations

To address the issues from the previous audit that have not been resolved, we now recommend that DCAS:

1. Require that all system users periodically change their passwords.

Agency Response: "This is an open issue. Previously, a decision had been made by the implementation team to forego the imposition of this control after considering the objections of the customer agency representatives and the other controls built into the MCMS system. We agree to revisit this issue with the customer agency personnel."

Auditor Comment: We strongly recommend that DCAS comply with Directive 18 and ensure that sufficient security controls are in place by having all system users periodically change their passwords.

2. Test the MCMS disaster recovery plan annually.

Agency Response: "We agree. We have contacted DoITT personnel who have assured us that MCMS will be a part of the annual test of their Disaster Recovery Plan. The next test is scheduled for January 23, 2003."

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 Internal Controls for the Department of Citywide Administrative Services' Data Center (7F02-166)

Dear Mr. Liwer:

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

First, we want to make it explicitly clear that this is a follow-up Audit of the *FAMIS* Data Center. FAMIS was a fleet management system which has since been eliminated, and the data center has been closed. At the current time, DCAS does not have its own data center.

Secondly, the report cites MCMS, the successor system to FAMIS, because the system controls do not require regularly scheduled password changes. Though the Comptroller's Directive 18 guidelines recommend this control, it was the opinion of the customer Agency fleet managers that this control would be disadvantageous. After considering the other controls built into the MCMS system, it was the decision of the implementation team to forego the imposition of this control.

As a result of this audit, DCAS will formally revisit this issue with the customer agencies.

Recommendations:

Recommendation 1: Require that all system users periodically change their passwords.

Response: This is an open issue. Previously, a decision had been made by the implementation team to forego the imposition of this control after considering the objections of the customer agency representatives and the other controls built into the MCMS system. We agree to revisit this issue with the customer agency personnel.

Recommendation 2: Test the MCMS Disaster Recovery Plan annually.

Response: We agree. We have contacted DoITT personnel who have assured us that MCMS will be a part of the annual test of their Disaster Recovery Plan. The next test is scheduled for January 23, 2003.

Thank you for the opportunity to comment on this report.

Very truly yours,

Martha K. Hirst