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

WILLIAM C. THOMPSON, JR.
Comptroller

Follow-Up Report on the New York City Fire Department Arson Information Management System Data Center

7F 02-161

May 31, 2002

Table of Contents

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

Follow-Up Audit Report on the New York City Fire Department Arson Information Management System Data Center

7F 02-161

SUMMARY OF FINDINGS AND CONCLUSIONS

This follow-up audit was conducted to evaluate the New York City Fire Department's (FDNY) progress in implementing the 22 recommendations made in an earlier audit, *Audit Report of the Internal Controls for the New York City Fire Department's Arson Information Management System Data Center* (Audit No. 7A95-140, issued January 4, 1996). The earlier audit evaluated the effectiveness of management's control over FDNY's Arson Information Management System (AIMS) data center in the areas of data and physical security, program change control, computer operations, and backup/contingency planning. In 1997, the Bureau of Fire Information Microcomputer System (BFIS) data center replaced the AIMS data center. In this follow-up audit, we discuss the recommendations made in the previous audit for the AIMS data center and how these recommendations have been addressed in the BFIS data center.

Our previous audit made 22 recommendations to FDNY. Of the 22 recommendations 15 were implemented, two were partially implemented, three were not implemented, and two are no longer applicable. The details of these recommendations and their implementation status follow. FDNY should:

1. "Establish security policies 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, which should address all administrative controls for monitoring the data center's security, its data integrity, its identification process efficiency, its recording of system access and changes." **IMPLEMENTED**

2. "Immediately identify all employees sharing passwords, and then comply with DOI's standard #210 by issuing programmer passwords on an individual basis." **IMPLEMENTED**

3. “Re-evaluate all existing user IDs, thereby eliminating unnecessary IDs (especially those assigned to individuals no longer employed by the FDNY) and/or excessive levels of system access for the given IDs.”
PARTIALLY IMPLEMENTED

4. “Comply with Comptroller’s Directive #18, requiring the changing of passwords regularly.” **IMPLEMENTED**

5. “Reassess the data center’s physical security in conjunction with the building’s owner, DGS.” **IMPLEMENTED**

6. “Require the data center’s staff to keep the entrance door to the data center locked at all times.” **IMPLEMENTED**

7. “Continue to require all visitors to sign a register if they do not work there.” **IMPLEMENTED**

8. “Provide guard service or an alarm system within the data center to prevent access by unauthorized persons. The greatest security is needed from 12:30 P.M to 7:30 A.M. when the center is unstaffed.” **IMPLEMENTED**

9. “Install a video camera to monitor the external doors.” **IMPLEMENTED**

10. “Seal the mail slot on the computer room’s external doors.” **IMPLEMENTED**

11. “Remove all reference to the center’s name on the front door nameplate.” **IMPLEMENTED**

12. “Comply with DOI’s Standard #511 by installing smoke/heat detectors immediately to ensure the safety of its assets and staff.” **NOT IMPLEMENTED**

13. “Continue to comply with DOI’s Standard #604 through consistent monitoring and maintenance of the AIMS fire extinguishers.” **IMPLEMENTED**

14. “Comply with DOI Standard #504 regarding emergency lighting within the data center.” **IMPLEMENTED**

15. “Develop, approve, and implement a Disaster Recovery/Contingency Plan in accordance with Comptroller’s Directive #18 and Department of Investigation Security Standards. This plan should include procedures for handling system emergencies that may occur during the hours that the facility is unstaffed.” **IMPLEMENTED**

16. "Test such a Disaster Recovery/Contingency Plan to ensure that it will provide smooth, rapid, and effective restoration of the data center's 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 in a real emergency." **NOT IMPLEMENTED**

17. "Comply with New York City Data Processing Standard #20.02 by removing all unnecessary equipment and articles from the computer room, cleaning under the raised floor, keeping the computer room tiles in place, and storing computer paper outside the computer room." **PARTIALLY IMPLEMENTED**

18. "Speed up the time table for the conversion or upgrading of the AIMS to protect it from system failure and to prevent loss of service to those depending on its data." **IMPLEMENTED**

19. "Adopt data center policies and procedures formally separating the programming and system functions. If the size of the data center's staff precludes this separation then AIMS management should establish compensating controls which will detect/prevent unauthorized changes to the AIMS operating system." **NOT IMPLEMENTED**

20. "Comply with the New York City Data Processing Standard #20." **NO LONGER APPLICABLE**

21. "Develop, approve, and implement policies, which ensure that all appropriate information is stored in the tape library, and that access is limited to prevent the loss or destruction of information." **IMPLEMENTED**

22. "Comply with New York City Data Processing Standard #20.14 by appointing a tape librarian who will be responsible for putting into practice the above policies and for conducting periodic physical inventories of the tape library." **NO LONGER APPLICABLE**

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

1. Identify and terminate inactive user accounts.

2. Install a smoke detector in the computer room.

3. Test the disaster recovery plan to ensure that it will provide a smooth, rapid, and effective restoration of the data center's functions. These tests should not be announced so that the staff learn how to function in a real emergency.

4. Remove unused equipment and tape cartridges from the computer room.

5. Develop and implement compensating controls to ensure that only authorized

changes are made to the system.

We conducted this follow-up audit 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 FDNY during and at the conclusion of this audit. A preliminary draft report was sent to FDNY officials to be discussed at an exit conference. FDNY officials stated that they agreed with the report findings and recommendations and that there was no need to hold an exit conference. On May 7, 2002, we submitted a draft report to FDNY officials with a request for comments. We received FDNY’s written response on May 22, 2002. FDNY said that it already implemented three of the five recommendations and plans to implement the other two recommendations.

The full text of FDNY’s comments is included as an addendum to this report.

INTRODUCTION

Background

The primary function of the New York City Fire Department (FDNY) is to protect life and property from fire. FDNY fulfills its responsibility by preventing, extinguishing, and investigating fires, and by educating the public about fire prevention. AIMS, the application that resided in the AIMS data center, was used to collect, organize, and distribute data required in the analysis, management, and reduction of arson-related incidents. In 1997, the Bureau of Fire Information Microcomputer System data center (BFI) replaced the AIMS data center and the Bureau of Fire Information System (BFIS) replaced AIMS. The AIMS network provided a citywide arson database serving eight user agencies at 23 remote sites; the BFIS network now provides this service. Users include: FDNY, the Police Department, the District Attorney's Office in each borough, the Arson Strike Force, and the New York State Office of Fire Prevention and Control. This follow-up audit evaluated whether the previous report's recommendations have been addressed in the new BFIS data center.

Objectives, Scope, and Methodology

This follow-up audit determined whether the 22 recommendations contained in a previous audit, *Audit Report of the Internal Controls for the New York City Fire Department Arson Information Management System Data Center* (Audit No. 7A 95-140, issued January 4, 1996) were implemented.

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

(1) Interviewed FDNY personnel,

(2) Reviewed and analyzed the data security controls,

(3) Toured the data center and determined whether FDNY implemented the physical and system security measures recommended in the previous audit,

(4) Reviewed and analyzed the FDNY disaster recovery plan, and

(5) Tested FDNY compliance with Directive #18.

The previous audit used the New York City Department of Investigation System Security Standards and the New York City Data Processing Standards as criteria; both of these standards have been rescinded. We have replaced those standards with the New York City Comptroller's Directive #18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems* and the Federal Information Processing Standards (FIPS) as criteria for our audits.

We conducted this follow-up audit 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 FDNY during and at the conclusion of this audit. A preliminary draft report was sent to FDNY officials to be discussed at an exit conference. FDNY officials stated that they agreed with the report findings and recommendations and that there was no need to hold an exit conference. On May 7, 2002, we submitted a draft report to FDNY officials with a request for comments. We received FDNY's written response on May 22, 2002. FDNY said that it already implemented three of the five recommendations, and plans to implement the other two recommendations.

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

OFFICE OF THE COMPTROLLER
NEW YORK CITY

DATE FILED: May 31, 2002

RESULTS OF THIS FOLLOW-UP AUDIT

Previous Finding: "FDNY's computerized assets and data are at risk due to the lack of protection from accidental or intentional destruction."

> ***Previous Recommendation #1:*** AIMS management should: "Establish security policies 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, which should address all administrative controls for monitoring the data center's security, its data integrity, its identification process efficiency, its recording of system access and changes."
>
> ***Previous Agency Response:*** "In view of the fact that the AIMS staff is small and experienced and has carried out its responsibilities adequately thus far, it is evident that the procedures in place are working. These procedures unfortunately are not written and they ought to be; however, due to the fact that AIMS will be phased out in the near future, it is not cost effective to assign a staff member to document the procedures that will soon be obsolete."

Current Status: IMPLEMENTED

BFI management provided standards that include policies for: the physical security of the data center, data security, access controls, and disaster recovery strategy. Therefore, we consider this recommendation implemented.

> ***Previous Recommendation #2:*** "Immediately identify all employees sharing passwords, and then comply with DOI's standard #210 by issuing programmer passwords on an individual basis."
>
> ***Previous Agency Response:*** **"**AIMS will comply. AIMS' programmers will be issued individual passwords by early January 1996."

Current Status: IMPLEMENTED

We received a list of all the staff members who have access to the BFIS system. We reviewed the list and found that all users receive unique log-in accounts and select their own passwords. Therefore, we consider this recommendation implemented.

****

Previous Finding: "Computer Data Access Control Weaknesses"

> ***Previous Recommendation #3:*** "Re-evaluate existing user IDs, thereby eliminating unnecessary IDs (especially those assigned to individuals no longer employed by the FDNY) and/or excessive levels of system access for the given IDs".

Previous Agency Response: **“**AIMS will comply. We will issue a directive to BFI and Payroll by February 1996, informing them of the requirement to eliminate unnecessary IDS.”

Current Status: PARTIALLY IMPLEMENTED

We found that FDNY employees were provided with the appropriate level of access to the system. However, four of 23 BFI users had retired (three of them in calendar year 2001) and, therefore, their user IDs should have been eliminated from the system. Accordingly, we consider this recommendation partially implemented.

Previous Recommendation #4: “Comply with Comptroller’s Directive #18, requiring the changing of passwords regularly.”

Previous Agency Response: **“**AIMS will comply. We will issue a directive to BFI and Payroll by February 1996, informing them of the requirement to . . . change passwords regularly. Upon receipt of their responses, we will implement the changes.”

Current Status: IMPLEMENTED

We found that BFI users are now required to change their passwords every 40 days. Therefore, we consider this recommendation implemented.

****

Previous Finding: “Inadequate Physical Security of AIMS’ Data Center puts the facility at risk.”

Previous Recommendation #5: “Reassess the data center’s physical security in conjunction with the building’s owner, DGS.”

Previous Agency Response: “BICS [Bureau of Information and Computer Services] will not comply with these recommendations because they are not reasonable given the circumstance of AIMS’ projected phase out.”

Current Status: IMPLEMENTED

The BFIS data center is now housed in a locked room on the fifth floor of a FDNY facility in Brooklyn. A coded keypad lock secures the fifth floor, and additional key locks secure the data center room and the server cabinet. Only two managers have access to the data center room. Fire Marshals on the fifth floor use a surveillance camera to monitor visitors. Therefore, we consider this recommendation implemented.

Previous Recommendation #6: “Require the data center’s staff to keep the entrance door to the data center locked at all times.”

Previous Recommendation #7: “Continue to require all visitors to sign a register if they do not work there.”

> ***Previous Agency Response:*** "AIMS is complying and will continue to do so; the entrance door is kept locked, visitors are required to sign a register."

Current Status: IMPLEMENTED

The entrance to the BFIS data center is kept locked. There is a visitor's log on the fifth floor where visitors sign in. Therefore, we consider Recommendations #6 and #7 implemented.

> ***Previous Recommendation #8:*** "Provide guard service or an alarm system within the data center to prevent access by unauthorized persons. The greatest security is needed from 12:30 P.M to 7:30 A.M. when the center is unstaffed."

> ***Previous Recommendation #9:*** **"**Install a video camera to monitor the external doors."

> ***Previous Agency Response:*** "BICS will not comply with these recommendation because it is unreasonable given the circumstance of AIMS' projected phase out."

Current Status: IMPLEMENTED

FDNY has a surveillance camera located in the front of the building where the data center is located, and there are two Fire Marshals who monitor a video console 24 hours a day, seven days a week. Therefore, we consider Recommendations #8 and #9 implemented.

> ***Previous Recommendation #10****:* "Seal the mail slot on the computer room's external doors."

> ***Previous Recommendation #11:*** "Remove all reference to the center's name on the front door nameplate."

> ***Previous Agency Response:*** **"**The mail slots on the computer room's external doors have been sealed, and explicit references to the data center and Fire Department have been removed from the front door nameplate. The letters 'AIMS' have been retained to enable the receipt of mail."

Current Status: IMPLEMENTED

Neither the entrance door to the fifth floor where the data center is housed nor the door to the data center room have mail slots, and there are no signs indicating that the data center is located in this area. Therefore, we consider recommendations #10 and #11 implemented.

****

Previous Finding: "FDNY does not have a fire detection system or an automatic extinguishing system."

Previous Recommendation #12: "Comply with DOI's Standard #511 by installing smoke/heat detectors immediately to ensure the safety of its assets and staff."

Previous Agency Response: "AIMS will comply. We will install smoke detectors in the computer room by January 16, 1996."

Current Status: NOT IMPLEMENTED

FDNY does not have smoke detectors inside the data center. Therefore, we consider this recommendation not implemented.

Previous Recommendation #13: "Continue to comply with DOI's Standard #604 through consistent monitoring and maintenance of the AIMS fire extinguishers."

Previous Agency Response: **"**AIMS will continue to comply."

Current Status: IMPLEMENTED

FDNY has a fire extinguisher located twenty feet from the front door of the data center. We verified that it is regularly maintained. Therefore, we consider the recommendation implemented.

Previous Recommendation #14: Comply with DOI Standard #504 regarding emergency lighting within the data center.

Previous Agency Response: "BICS will not comply with this recommendation because it is not cost effective in view of the projected phase out of AIMS."

Current Status: IMPLEMENTED

FDNY now has emergency lighting within the data center. Therefore, we consider this recommendation implemented.

****

Previous Finding: "AIMS has neither an automated backup facility nor a formally approved disaster recovery plan."

Previous Recommendation #15: "Develop, approve, and implement a Disaster Recovery/Contingency Plan in accordance with Comptroller's Directive #18 and Department of Investigation Security Standards. This plan should include procedures for handling system emergencies that may occur during the hours that the facility is unstaffed."

Current Status: IMPLEMENTED

FDNY developed a Disaster Recovery/Contingency Plan for restoring BFIS in the event the data center becomes inoperable. Therefore, we consider this recommendation implemented.

Previous Recommendation #16: "Test such a Disaster Recovery/Contingency Plan to ensure that it will provide smooth, rapid, and effective restoration of the data center's 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 in a real emergency."

Previous Agency Response: **"**BICS will not comply with these recommendations. To compile a formal comprehensive Disaster Recovery/Contingency Plan requires a major effort in terms of time and staffing. Given the circumstances of the expected termination of AIMS, this would not be cost effective. The Fire Department is nevertheless concerned about ensuring continuity of AIMS operations in the event of a disaster. Therefore, BICS has addressed the most important component in disaster recovery, namely protecting the data. This has been accomplished by off-site storage of the AIMS data tapes in the BICS tape library. Furthermore, we are aware of sources for replacement hardware if that should be necessary. Relevant notes on the subject of recreating AIMS in an emergency will be included as an addendum to our BICS Disaster Recovery Plan. The testing of a Disaster Recovery/Contingency Plan implies the use of an alternative-processing site. We do not have the availability of such a site and contracting for the service would be an unwarranted expense. The recommendation is therefore, impractical."

Previous Auditors' Response: "In [a prior] Comptroller's Audit Report of the BICS data center, we noted that BICS has neither an automated backup facility nor a formally approved disaster recovery plan. Furthermore, BICS does not have adequate control over its tape library. The FDNY indicated that they have taken steps to correct this situation but we have not yet been informed whether this situation has been alleviated."

Current Status: NOT IMPLEMENTED

BFI has not tested its disaster recovery plan. Comptroller's Directive §10-4 states:

> "Periodic reviews and updates are necessary to ensure that the business continuation plan remains current. Comprehensive tests should be conducted annually."

Therefore, we consider this recommendation not implemented.

****

Previous Finding: AIMS administrative and operating controls need improvement."

> ***Previous Recommendation #17:*** "Comply with New York City Data Processing Standard #20.02 by removing all unnecessary equipment and articles from the computer room, cleaning under the raised floor, keeping the computer room tiles in place, and storing computer paper outside the computer room."
>
> ***Previous Agency Response:*** **"**AIMS will comply to the extent feasible. General good housekeeping practices in the computer room will begin immediately. The removal of unnecessary equipment and articles will be accomplished by mid-January 1996. We will explore the practicability of contracting a professional computer room cleaner to clean under the raised floor. The paper stored in the closet will remain. All floor tiles that can be put in place without disturbing the computer wiring will be reinstalled."

Current Status: PARTIALLY IMPLEMENTED

The new computer room does not have a raised floor, so the previous recommendation regarding cleaning under the raised floor is no longer applicable. FDNY no longer stores paper in the data center. However, unnecessary equipment is still being stored in the data center, including two uninstalled UPS devices, eight uninstalled modems, one zip drive, and 10 tape cartridges. Therefore, we consider the recommendation partially implemented.

> ***Previous Recommendation #18:*** "Speed up the time table for the conversion or upgrading of the AIMS to protect it from system failure and to prevent loss of service to those depending on its data."
>
> ***Previous Agency Response:*** "BFI is developing a new system for the AIMS Function using modern hardware. The planned takeover by BFI of the AIMS function is expected in June 1996."

Current Status: IMPLEMENTED

AIMS has been converted to BFIS; BFIS information is stored on a network, and all issues related to system failure and loss of service have been addressed. Therefore, we consider the recommendation implemented.

> ***Previous Recommendation #19:*** "Adopt data center policies and procedures formally separating the programming and system functions. If the size of the data center's staff precludes this separation, then AIMS management should establish compensating controls which will detect/prevent unauthorized changes to the AIMS operating system."
>
> ***Previous Agency Response:*** **"**AIMS will comply to the extent feasible. As the auditors note, the AIMS center is a small shop in which formal separation of programming and system functions is impractical. As a compensating control we will issue a directive that each programmer submit any programming or system changes he performs to another

programmer for approval. The approved changes will be documented and kept on file. This will provide accountability for their work any related errors."

Current Status: NOT IMPLEMENTED

FDNY still assigns both programming and system functions to one individual. BFIS is a much smaller system than AIMS, and therefore it may not be practical to segregate these functions. Nevertheless, as stated in the previous audit, if FDNY determines that it is not feasible to separate these functions, it needs to implement compensating controls to ensure that only authorized changes are made to the system. For example, FDNY could require other data center personnel to review and approve all system changes initiated by the agency's administrator/programmer. Accordingly, we consider the recommendation not implemented.

Previous Recommendation #20: "Comply with the New York City Data Processing Standard #20."

Previous Agency Response: **"**BICS will comply to the extent feasible given the circumstance of the projected termination of AIMS."

Current Status: NO LONGER APPLICABLE

This recommendation is no longer applicable because the New York City Data Processing Standards have been rescinded by the Mayor's Office.

****

Previous Finding: "AIMS does not have adequate control over its tape library; this is needed to ensure that critical data is not misplaced or lost."

Previous Recommendation #21: "Develop, approve, and implement policies which ensure that all appropriate information is stored in the tape library, and that access is limited to prevent the loss or destruction of information."

Previous Agency Response: "AIMS is complying and will continue to do so. AIMS' tapes have been delivered to the BICS tape library. As the need arises, additional tapes will be brought there for secure storage. Although BICS does not have a formal tape librarian, the duties of the tape librarian are shared by the operations manager and a computer aide. These duties include restricting access to the tapes and periodically conducting physical inventories."

Current Status: IMPLEMENTED

BFI has developed policies to ensure that all appropriate information is secured to prevent the loss or destruction of information. Therefore, we consider this recommendation implemented.

Previous Recommendation #22: "Comply with New York City Data Processing Standard #20.14 by appointing a tape librarian who will be responsible for putting into practice the above policies and for conducting periodic physical inventories of the tape library."

Previous Agency Response: "AIMS is complying and will continue to do so. AIMS' tapes have been delivered to the BICS tape library. As the need arises, additional tapes will be brought there for secure storage. Although BICS does not have a formal tape librarian, the duties of the tape librarian are shared by the operations manager and a computer aide. These duties include restricting access to the tapes and periodically conducting physical inventories." [Same response applies to Recommendations #21 and #22.]

Current Status: NO LONGER APPLICABLE

BFIS is a real-time database that does not require the use of tapes. Therefore, we consider this recommendation no longer applicable.

Recommendations

We recommend that FDNY BFI management:

1. Identify and terminate inactive user accounts.

   Agency Response: "AGREE – Inactive user accounts have already been terminated from the system. All accounts will be reviewed on a regular basis by the system administrator, and any additional inactive users accounts will be terminated as they occur."

2. Install a smoke detector in the computer room.

   Agency Response: "AGREE – A smoke detector was installed in the computer room on May 20, 2002."

3. Test the disaster recovery plan to ensure that it will provide a smooth, rapid, and effective restoration of the data center's functions. These tests should not be announced so that the staff learns how to function in a real emergency.

   Agency Response: "AGREE – Periodic unannounced tests of the disaster recovery plan will be performed, and any deficiencies in the plan will be identified and corrected."

4. Remove unused equipment and tape cartridges from the computer room.

Agency Response: “AGREE – All unused equipment and tape cartridges have been removed from the computer room, and periodic inspections of the room will be performed by the system administrator to ensure future compliance.”

5. Develop and implement compensating controls to that ensure only authorized changes are made to the system.

Agency Response: “AGREE – FDNY is in the process of developing such controls to ensure that only authorized changes are made to the system.”

The City of New York

FIRE DEPARTMENT
9 METROTECH CENTER BROOKLYN, N.Y. 11201-3857

DAVID CLINTON
Deputy Fire Commissioner
Legal Affairs

Room 8N-7

May 22, 2002

Roger D. Liwer
Assistant Comptroller for Audits
Office of the Comptroller
1 Center Street Room 1100
New York, N.Y. 10007-2341

Re: Follow-up Audit Report on the New York City Fire Department Arson Information Management System (AIMS) Data Center [7F02-161]

Dear Mr. Liwer:

The Fire Department has reviewed the follow-up audit report from the Office of the Comptroller on the AIMS Data Center. Our response to each of the five recommendations made by the Comptroller's Office is as follows:

1) **Recommendation – Identify and terminate inactive user accounts.**

   FDNY Response – AGREE – Inactive user accounts have already been terminated from the system. All accounts will be reviewed on a regular basis by the system administrator, and any additional inactive user accounts will be terminated as they occur.

2) **Recommendation – Install a smoke detector in the computer room.**

   FDNY Response – AGREE – A smoke detector was installed in the computer room on May 20, 2002.

3) **Recommendation – Test the disaster recovery plan to ensure that it will provide a smooth, rapid, and effective restoration of the data center's functions. These tests should not be announced so that the staff learn how to function in a real emergency.**

   FDNY Response – AGREE – Periodic unannounced tests of the disaster recovery plan will be performed, and any deficiencies in the plan will be identified and corrected.

4) **Recommendation – Remove unused equipment and tape cartridges from the computer room.**

   FDNY Response – AGREE – All unused equipment and tape cartridges have been removed from the computer room, and periodic inspections of the room will be performed by the system administrator to ensure future compliance.

5) **Recommendation – Develop and implement compensating controls to ensure that only authorized changes are made to the system.**

   FDNY Response – AGREE – FDNY is in the process of developing such controls to ensure that only authorized changes are made to the system.

The Fire Department would like to express our thanks to you and your staff for the assistance that you have given us in improving the Department.

Very truly yours,

David Clinton

David Clinton

DC:dd