

# AUDIT REPORT



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

## **Second Follow-up Audit Report on Department of Education Internal Controls Over Its Data Center**

*7F04-137*

**September 27, 2004**



THE CITY OF NEW YORK  
OFFICE OF THE COMPTROLLER  
1 CENTRE STREET  
NEW YORK, N.Y. 10007-2341

WILLIAM C. THOMPSON, JR.  
COMPTROLLER

**To the Citizens of the City of New York**

Ladies and Gentlemen:

In accordance with the responsibilities of the Comptroller contained in Chapter 5, §93, of the New York City Charter, my office has reviewed the implementation status of 12 recommendations made in a previous audit entitled, Follow-up Audit Report of the Internal Controls of the Board of Education's Data Center (Audit # 7F01-113, issued May 8, 2001).

The results of our audit, which are presented in this report, have been discussed with Department of Education officials, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that City agencies have adequate controls, procedures, and policies in place to protect their computer operations from inappropriate access and use.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please contact my Audit Bureau at 212-669-3747 or e-mail us at [audit@Comptroller.nyc.gov](mailto:audit@Comptroller.nyc.gov).

Very truly yours,

A handwritten signature in cursive script that reads "William C. Thompson, Jr.".

William C. Thompson, Jr.

WCT/gr

**Report:** 7F04-137  
**Filed:** September 27, 2004

## *Table of Contents*

<b>AUDIT REPORT IN BRIEF</b>	1
<b>INTRODUCTION</b>	2
Background	2
Objectives	2
Scope and Methodology	3
Discussion of Audit Results	3
<b>RESULTS OF FOLLOW-UP AUDIT</b>	3
<b>NEW FINDINGS AND RECOMMENDATION</b>	11
<b>ADDENDUM</b> Department of Education Response	

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

**Second Follow-up Audit Report on  
Department of Education Internal Controls  
Over Its Data Center**

**7F04-137**

---

**AUDIT REPORT IN BRIEF**

This second follow-up audit determined whether the Department of Education (DOE), formally the Board of Education (the Board), implemented the 12 recommendations made in an earlier audit, *Follow-up Audit Report of the Internal Controls of the Board of Education's Data Center* (Audit 7F01-113, issued May 8, 2001). We conducted this second follow-up audit because issues reported in our initial audit of the Board's Data Center, *Audit Report of the Internal Controls of the Board of Education's Data Center*, (Audit 7A95-172, Issued June 15, 1995), had not been fully resolved and since a new issue was disclosed in the follow-up audit.

The first follow-up audit found a number of weaknesses, including that the data center did not have an alternate-processing site and did not complete, formally approve, and update its disaster recovery plan. In addition, the Board did not have a time-out function to limit computer access during extended periods of inactivity; did not have a method to detect unauthorized hardware and software use on its networks; and had not conducted penetration testing of its computer networks. Moreover, the Board had insufficient Internet connectivity security controls and did not monitor firewall traffic sufficiently. In this audit, we discuss the 12 recommendations we made in the first follow-up report as well as the implementation status of those recommendations.

**Audit Findings and Conclusions**

DOE implemented one, partially implemented two, and did not implement nine of the 12 recommendations made in the previous audit. In this second follow-up audit, we found that DOE has installed time-out features for all on-line systems and has installed Internet security software to monitor the Internet activities of the instructional staff and to generate associated reports. To control access to undesirable Web sites, DOE has installed filtering software on all

servers used for instructional purposes within schools. However, DOE still has not established sufficient Internet security controls for its administrative staff, does not conduct regular penetration testing of its computer networks, and does not monitor its firewall traffic. Moreover, DOE still has not established procedures to detect unauthorized hardware and software use on its networks.

In addition, DOE still does not have an alternate-processing site to resume data processing operations in the event of a disaster, nor a complete, formally approved, tested, or updated disaster recovery plan. However, DOE will consolidate its mainframe computer operations with those of the Department of Information Technology and Telecommunications (DoITT) by the end of calendar year 2004. Although DoITT will perform disaster recovery for DOE mainframe computer operations after the consolidation, DOE will continue to be responsible for its network disaster recovery.

Other issues identified during this audit included weaknesses in system access controls and procedures.

## **INTRODUCTION**

### **Background**

DOE provides primary and secondary education to approximately one million students, from pre-kindergarten to grade 12, in approximately 1,200 schools. DOE projects that for the 2005 school year that it will employ 108,348 full-time pedagogical employees—teachers, superintendents, principals, assistant principals, guidance counselors, school secretaries, educational paraprofessionals, and other school support staff—approximately 77,000 of whom are teachers who prepare students to meet grade-level standards in reading, writing, and mathematics, and to prepare high school students to pass the Regents exams and to meet graduation requirements.

DOE's Division of Instructional and Information Technology (DIIT) provides innovative information and resource-management tools to support the instruction throughout DOE. DIIT is responsible for managing DOE computer equipment, developing and supporting software applications, and operating the data center.

### **Objectives**

The objective of this audit was to determine whether DOE implemented the 12 recommendations made in an earlier report, *Follow-up Audit Report of the Internal Controls of the Board of Education's Data Center* (Audit # 7F01-113, issued May 8, 2001).

## **Scope and Methodology**

This audit covered the period March through May 2004. To determine the implementation status of the recommendations as well as the adequacy of system access controls and procedures, we:

- toured the data center;
- interviewed DOE personnel;
- reviewed and analyzed password controls and procedures;
- reviewed network and mainframe user profiles;
- reviewed and analyzed security procedures for Internet and system access; and
- tested DOE compliance with Directive 18 and applicable *Federal Information Processing Standards* (FIPS) and the Department of Investigation's *Information Security Directive*.

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

## **Discussion of Audit Results**

The matters covered in this report were discussed with DOE officials during and at the conclusion of this audit. A preliminary draft was sent to DOE officials and discussed at an exit conference held on June 7, 2004. On June 9, 2004, we submitted a draft report to DOE officials with a request for comments. We received a written response from the Department on June 22, 2004. In its response, DOE agreed with 10 of the 12 recommendations made in this audit. The two recommendations that DOE disagreed with relate to additional Internet security for administrative staff.

The full text of the DOE response is included as an addendum to this final report.

## RESULTS OF FOLLOW-UP AUDIT

**Previous Finding:** “The Board . . . does not have an alternate-processing site, which would enable the Board to resume mission-critical data processing operations in the event of a disaster at the Data Center.”

***Previous Recommendation #1:*** “Establish an alternate-processing site that should serve as a back-up site in the event of a Data Center disaster.”

***Previous Recommendation #2:*** “Prepare and equip the alternate-processing site so that the Board could resume mission-critical data processing operations in the event of a Data Center disaster.”

***Previous DOE Response to Recommendation #1 and #2:*** “Based on the current use of our Data Center and the tremendous cost of redundancy for an off-site backup location, the NYC-BOE’s DIIT has consciously opt[ed] not to establish a ‘hot’ backup site for our Data Center at this point in time. The current use of the BOE’s Data Center for critical applications can easily be backed-up in a manual mode for some period of time, without loss of support of our primary function, educating students.

“There are manual backup procedures for the critical functions currently performed by the systems at our Data Center, and these will suffice in case of a disaster or emergency. Henc[e], it is determined that a ‘hot’ backup site is not cost effective for the NYC-BOE as it would not directly affect its primary purpose, educating students. As such, we have completed this recommendation of this audit.”

### **Current Status of Recommendation # 1 and #2:** NOT IMPLEMENTED

DOE still does not have an alternate-processing site that would serve as a backup site to resume mission-critical data processing operations in the event of a disaster. According to agency officials, DOE will consolidate its mainframe computer operations with those of DoITT by the end of calendar year 2004. After the consolidation, DoITT will provide an offsite disaster recovery with an outside vendor and data backup services. However, DOE still needs an alternative-processing site to resume its network computer operations in the event of a disaster. We therefore consider recommendations #1 and #2 not implemented.

### **Recommendations**

The DOE should:

1. Establish an alternate-processing site that would serve as a back-up site in the event of a disaster.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is pending, as follows: “DOE is in the process of consolidating its mainframe computer operations with New York City’s Department of Information Technology and Telecommunications by mid-February 2005. When consolidation is completed, the DOE mainframe computer operations will have been merged with DoITT’s and will be included in DoITT’s disaster recovery processes which include off-site disaster recovery locations. Also, the DOE is currently re-architecting its network infrastructure using SONET ring technology scheduled for completion by the beginning of calendar year 2005. At that time, the SONET ring architecture consisting of 7 nodes will be ‘self healing’ and the network will be operational if any node is disabled. In essence, this technology will provide for seven ‘disaster recovery’ sites. In the Data Center Consolidation plan, our server consolidation will have a disaster recovery component.”

2. Prepare and equip the alternate-processing site so that DOE could resume mission-critical data processing operations in the event of a data center disaster.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is pending, as follows: “Once consolidation of the computer operations is completed with DoITT, all processes will be in place for disaster recovery as the DOE operations will be covered by the existing DoITT Disaster Recovery processes. As we consolidate with DoITT, we will also be developing disaster recovery plans along with our plans for server consolidation.”

**Previous Finding:** “The Board has a formal disaster recovery plan. However, this plan is incomplete and has not yet been approved.”

**Previous Recommendation #3:** “Complete and formally approve its disaster recovery plan.”

**Previous DOE Response:** “The plan is undergoing review by the CIO and the Director of Data center before being approved.”

**Previous Finding:** “The Board does not conduct regular reviews, and has not fully tested its disaster recovery/contingency plan.”

**Previous Recommendation #4:** “Conduct a comprehensive test of the disaster recovery plan, which should be followed, by a similar test once a year every year.”

**Previous DOE Response:** “DIIT’s Data Center has conducted partial tests of its disaster recovery plan in that the restore procedures have been used periodically to recover from applications, system, or hardware problems. It is not practical to do a comprehensive test without an off-site facility since it would involve



restoring many, many backups over our existing production volumes which could cause problems in itself, and be extremely time consuming.”

**Previous Recommendation #5:** “Update the disaster recovery plan when the information it contains becomes obsolete.”

**Previous DOE Response:** “The plan is undergoing review by the CIO and the Director of Data center before being approved. It is also planned that the Board will do annual review and update once the plan is approved.”

**Current Status of Recommendations #3, #4, and #5: NOT IMPLEMENTED**

DOE still does not have a complete, formally approved, tested, or updated disaster recovery plan. Although DoITT will provide a disaster recovery plan for its mainframe computer operations after the consolidation, DOE will continue to be responsible for its network disaster recovery. DOE should have a comprehensive disaster recovery plan to ensure the timely and efficient resumption of operations in the event of a disaster. Therefore, we consider recommendations #3, #4, and #5 not implemented.

**Recommendations**

The DOE should:

3. Complete and formally approve its disaster recovery plan.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is pending, as follows: “Once consolidation with DoITT has been completed, DoITT’s Disaster Recovery plan, as it relates to DOE functionality, will be reviewed and approved by DOE management. As we consolidate with DoITT, we will also be developing disaster recovery plans along with out plans for server consolidation.”

4. Conduct a comprehensive test of the disaster recovery plan, which should be followed by a similar test once a year, every year.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is pending, as follows: “Once consolidation with DoITT is completed by the end of calendar 2004, the DOE will participate in all DoITT’s Disaster Recovery tests which occur twice annually. As we consolidate with DoITT, we will also be developing disaster recovery plans along with out plans for server consolidation.”

5. Update the disaster recovery plan when the information it contains becomes obsolete.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is pending, as follows: “We will update the existing disaster recovery plan and merge with DoITT’s disaster recovery plan as it relates to DOE functionality once consolidation is complete with DoITT. DOE will be full participants in the testing of DoITT’s Disaster

Recovery program. DOE's disaster recovery plan will be further updated at the completion of the server consolidation."

**Previous Finding:** "The Board installed the time-out feature on its Employee Information System, Automate the Schools system, Child Assistance Program system, and TBANK payroll information system. The Board, however, has not installed this feature on its Custodial Payroll system, Financial Accounting Management Information Systems, and Galaxy budget system."

**Previous Recommendation #6:** "Implement time-out features for the Financial Accounting Management Information System, the Custodial Payroll System, and the Galaxy computer system."

**Previous DOE Response:** "FAMIS [Financial Accounting Management Information System] and the Custodial Payroll Systems application programmers will implement, with DIIT's assistance, a time-out feature in both systems by December 31, 2001."

"By June 30, 2001 all schools participating in Galaxy will have a time-out feature. District offices time-out feature will be operational by December 31, 2001."

**Current Status:** IMPLEMENTED

DOE has installed the time-out features for all on-line systems. We therefore consider Recommendation #6 implemented.

**Previous Finding:** "The Board does not have a method to detect unauthorized hardware . . . and unauthorized software that could threaten the Board's computerized networks by unauthorized individuals." In addition, the Board has not conducted penetration testing of its computer networks; has not implemented sufficient Internet connectivity security controls; and, does not sufficiently monitor its firewalls.

**Previous Recommendation #7:** "Establish and implement procedures for using polling software to catalog and monitor individual workstation hardware and software."

**Previous Recommendation #8:** "Conduct regular penetration testing of its computer networks and document the results. In addition, the Board's Internet security should be updated, as needed, based on the result of the penetration testing."

**Previous DOE Response to Recommendation #7 and #8:** "The Board recognizes the benefits of this function and as the Board continues to develop its security

measures, pending availability of competing resources, this recommendation will be addressed.”

***Previous Recommendation #9:*** “Establish and implement Internet security procedures for generating web server statistics on all web-related activities, including all websites accessed by the Board’s staff.”

***Previous Recommendation #10:*** “Establish and implement Internet security procedures for scanning all web-related activity for unusual or suspicious activities.”

***Previous DOE Response to Recommendation #9 and #10:*** “The Board formally approved a comprehensive Internet Acceptable Use Policy (IAUP) in February 2001. This IAUP will be the guideline for all Board’s staff.”

***Previous Recommendation #11:*** “Establish and implement Internet security procedures for using filtering software to control access to undesirable websites by Board staff.”

***Previous DOE Response to Recommendation 11:*** “While the Board does utilize content-filtering software to monitor instructional usage of the network and Internet it has made a decision not to utilize filtering software for administrative users. We feel that the Internet Acceptable Use Policy (IAUP), and staff management, is sufficient to provide the direction and enforcement required.”

***Previous Recommendation #12:*** “Establish and implement procedures for monitoring all inbound and outbound traffic passing through the firewalls.”

***Previous DOE Response to Recommendation 12:*** “While Firewalls logs are maintained for a short period of time, additional funding will be required to acquire the necessary hardware that will enable the long-term historical archiving of this data. In addition, pro-active monitoring of this information can not be accommodated because of current staffing issues.”

**Current Status of Recommendation #7 and #8: NOT IMPLEMENTED**

DOE still has not established procedures for using polling software to catalog and monitor individual workstation hardware and software. Further, DOE still does not conduct regular penetration testing of its computer networks, document the results, and update the Internet security based on the result of penetration testing. Therefore we consider recommendation #7 and #8 not implemented.

## **Recommendations**

The DOE should:

6. Establish and implement procedures for using polling software to catalog and monitor individual workstation hardware and software.

***DOE Response:*** DOE stated that it agrees with the recommendation, but implementation is pending, as DOE “recognizes the benefits of this function and now had created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.”

7. Conduct regular penetration testing of its computer networks and document the results. In addition, DOE Internet security should be updated, as needed, based on the result of the penetration testing.

***DOE Response:*** DOE stated that it agrees with the recommendation, but implementation is pending the availability of funding. Specifically, DOE stated that it: “recognizes the benefits of this function and now had created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.”

## **Current Status Recommendation #9: PARTIALLY IMPLEMENTED**

DOE has installed Internet security software to monitor the Internet activities of the instructional staff and to generate associated reports. However, the security software does not currently monitor the Internet activities for the administrative staff. We therefore consider recommendation #9 partially implemented.

## **Recommendation**

8. The DOE should establish and implement Internet security procedures for generating Web server statistics on all Web-related activities, including all Web sites accessed by the administrative staff.

***DOE Response:*** DOE disagrees with the recommendation and stated that: “DOE has over 130,000 administrative employees. To implement a plan to filter all administrative workstations would be cost prohibitive and difficult to monitor. The DOE maintains its policy of active supervision by administrative managers, directors, and supervisors.”

***Auditor Comment:*** DOE’s response does not make sense. Since the software has already been installed on DOE’s computer network, and it already monitors the actions of over 91,000 of its 130,000 employees, we question why it believes that it would be cost prohibitive and difficult to monitor the remaining staff.

**Current Status Recommendation #10: NOT IMPLEMENTED**

DOE still has not established Internet security procedures for scanning all Web-related activity for unusual or suspicious activities. We therefore consider recommendation #10 not implemented.

**Recommendation**

9. The DOE should establish and implement Internet security procedures for scanning all Web-related activity for unusual or suspicious activities.

***DOE Response:*** DOE stated that it agrees with the recommendation, but implementation is pending available funding. Specifically, DOE stated that it: “recognizes the benefits of this function and now had created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.”

**Current Status Recommendation #11: PARTIALLY IMPLEMENTED**

DOE has installed filtering software to control access to undesirable Web sites on all servers used for instructional purposes within schools. However, DOE has not established similar Internet security controls at administrative workstations. We therefore consider recommendation #11 partially implemented.

**Recommendation**

10. The DOE should establish and implement Internet security procedures for using filtering software to control access to undesirable Web sites by administrative staff.

***DOE Response:*** DOE disagrees with the recommendation and stated that: “DOE has over 130,000 administrative employees. To implement a plan to filter all administrative workstations would be cost prohibitive and difficult to monitor. The DOE maintains its policy of active supervision by administrative managers, directors, and supervisors.”

***Auditor Comment:*** Again, DOE’s response does not make sense. As previously stated, the software has already been installed on DOE’s computer network, and it already monitors the actions of over 91,000 of its 130,000 employees. Therefore, we question why DOE believes that it would be cost prohibitive and difficult to monitor the remaining staff.

**Current Status Recommendation #12: NOT IMPLEMENTED**

DOE still has not established procedures for monitoring all inbound and outbound traffic passing through the firewalls. Therefore, we consider recommendation #12 not implemented.

## **Recommendation**

11. The DOE should establish and implement procedures for monitoring all inbound and outbound traffic passing through the firewalls.

**DOE Response:** DOE stated that it agrees with the recommendation, but implementation is available funding. Specifically, DOE stated that it: “recognizes the benefits of this function and now had created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.”

## **NEW FINDINGS AND RECOMMENDATION**

While determining whether our prior recommendation concerning time-out features for all on-line systems was implemented we found deficiencies in DOE’s other system access controls that should be corrected.<sup>1</sup> Specifically, DOE does not have written password policies and procedures for protecting the integrity of passwords on its networks; it does not require that users periodically change their passwords; and it does not ensure that passwords are adequately controlled.

Directive 18, § 8.1.2, states: “user identifications and passwords are among the most widely used and visible forms of access controls . . . Passwords control the applications or system information an individual is permitted to access.” § 8.1.2 further states that “active password management includes:

- (1) Insuring that users are forced to change passwords periodically;
- (2) Limiting the reuse of passwords;
- (3) Deactivation of inactive user accounts and accounts for employees whose services have terminated; and
- (4) The dissemination of a written policy that provides user guidance for protecting the integrity of passwords.”

We found that 4,194 of 17,000 mainframe user-IDs have never logged onto the system and 3,570 mainframe user-IDs and passwords were unused for more than 120 days. Despite having never been used or being unused for extended periods of time, DOE has not disabled or deleted these user-IDs and passwords.

---

<sup>1</sup> The time-out feature is a basic access control that is used to protect the information processing environment

In addition, we found that 98 former employees still had active mainframe access after leaving DOE. Those individuals were listed on the City Payroll Management System database as no longer employed or on leave. (Subsequent to the exit conference, DOE deleted mainframe access of 27 of the 98 former employees; it is reviewing the status of the remaining individuals.) Finally, we found 6,635 duplicated user-IDs on the mainframe user-ID list. Neglecting to delete duplicate user-IDs burdens the system with maintaining excess information and reduces the system's response time, thereby hindering user productivity.

### **Recommendation**

12. DOE should ensure that it actively manages system passwords. In this regard DOE should develop written password policies for its networks. These policies should require users to periodically change their passwords and include procedures for reviewing the status of inactive user-IDs and terminating them, as appropriate.

***DOE Response:*** DOE stated that the recommendation has been partially implemented. Specifically, DOE stated that: "27 of the 98 IDs have been deleted from the list of IDs identified during the audit as being former employees. 21 of the 98 IDs are being reviewed and appear to be active consultants. 50 of the 98 IDs have been found to be active employees. Of the 6,635 IDs found to be duplicates, none are actually duplicates as the analysis appeared to compare only 4 characters of the IDs whereas many IDs have more than 4 characters. We have begun to actively remove IDs for accounts not accessed for 120 days. We have also implemented a 90 day password change policy for Outlook e-mail accounts and have begun to develop written policies and procedures which will also be in effect for mainframe passwords."



# THE NEW YORK CITY DEPARTMENT OF EDUCATION

JOEL I. KLEIN, *Chancellor*

ADDENDUM

Page 1 of 14

## OFFICE OF THE DEPUTY CHANCELLOR

Kathleen Grimm, Deputy Chancellor for Finance and Administration

52 Chambers Street, Room 320 • New York, New York 10007

(212) 374-0209 (Voice) (212) 374-5588 (Facsimile)

June 22, 2004

Mr. Greg Brooks  
Deputy Comptroller  
The City of New York  
Office of the Comptroller  
1 Centre Street  
New York, N. Y. 10007-2341

Re: Second Follow-up Audit Report on  
Department of Education Internal Controls  
Over Its Data Center 7F04-137

Dear Mr. Brooks:

Enclosed is the NYC Department of Education's (DOE) Division of Instructional and Information Technology (DIIT) response/comments to the above draft audit report.

DIIT basically agrees with recommendations 1-7, 9, and 11 and has started implementing recommendation 12. DIIT disagrees with recommendations 8 and 10.

As detailed in the attached Audit Implementation Plan Forms, the disaster recovery processes within the DOE will be handled with the consolidation of our mainframe computer operations with those of the New York City Department of Information Technology and Telecommunications, along with the re-architecture of the DOE network into a fault tolerant SONET ring architecture, both planned for the beginning of calendar year 2005.

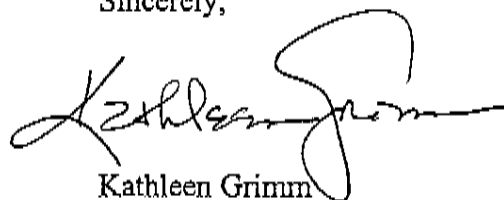
The DOE agrees with most of the security recommendations, and as such, is in the process of expanding its security office to further its ability to examine and strengthen the DOE's security procedures. As funding becomes available, the DOE will be able to accomplish the recommendations identified in this audit. However, the DOE disagrees with the recommendations for additional internet security for administrative staff as the recommendations are cost prohibitive and we feel that the active supervision of this staff by administrative managers, directors, and supervisors is adequate without unnecessarily impeding on the work function of the administrative staff.



Although the DOE agrees with the recommendations for more active management of its IDs and passwords, we disagree with some of the related findings. Specifically, the DOE disables its passwords within 45 days of inactivity and revokes usage at 120 days. Although these IDs and passwords remain on the database, they cannot be used to access DOE's systems. Also, the DOE system does not allow for duplicate IDs and we believe that the finding was based on a 4-character ID comparison whereas the IDs used by DOE can have more than 4 characters.

Additionally, of the 98 former employees identified on our security database, 27 have been deleted, 21 are still under reviewed and appear to be consultants and the remaining 50 are active employees.

Sincerely,



Kathleen Grimm

Deputy Chancellor for Finance and  
Administration

KG:sn

Enclosures

C:	Joel I. Klein	LaVerne Srinivasan	Maureen Hayes
	Michele Cahill	Carmen Farina	Bruce Feig
	Michael Best	Charles Niessner	Steve Vigilante
	Joe Eaione	Dan Moy	Rick Stewart
	Brian Fleischer	Marlene Malamy	Steven Neuman
	Nader Francis		

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

1. Establish an alternate processing site that would serve as a backup site in the event of a disaster.

**RESPONSE TO RECOMMENDATION**

As provided to the auditor, the DOE is in the process of consolidating its mainframe computer operations with New York City's Department of Information Technology and Telecommunications by mid-February 2005. When consolidation is completed, the DOE mainframe computer operations will have been merged with DoITT's and will be included in DoITT's disaster recovery processes which include off-site disaster recovery locations. Also, the DOE is currently re-architecting its network infrastructure using SONET ring technology scheduled for completion by the beginning of calendar year 2005. At that time, the SONET ring architecture consisting of 7 nodes will be "self healing" and the network will be operational if any node is disabled. In essence, this technology will provide for seven "disaster recovery" sites. In the Data Center Consolidation plan, our server consolidation will have a disaster recovery component.

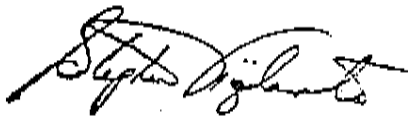
**TARGET IMPLEMENTATION DATE**

Completion of consolidation with DoITT is scheduled for mid-February 2005. Completion of the SONET ring is scheduled for the beginning of calendar year 2005. We expect to implement the server consolidation disaster recovery plan by end of calendar year 2005.

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

Print Name:

6/17/04

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

2. Prepare and equip the alternate processing site so that DOE could resume mission critical data processing operations in the event of a data center disaster.

**RESPONSE TO RECOMMENDATION**

As noted above, once consolidation of the computer operations is completed with DoITT, all processes will be in place for disaster recovery as the DOE operations will be covered by the existing DoITT Disaster Recovery processes. As we consolidate with DoITT, we will also be developing disaster recovery plans along with our plans for server consolidation.

**TARGET IMPLEMENTATION DATE**

It is our intent to have mainframe computer disaster recovery completed by mid-February 2005 and a server disaster recovery plan in place by the end of calendar 2005.

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_\_ OF \_\_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

3. Complete and formally approve its disaster recovery plan.

**RESPONSE TO RECOMMENDATION**

Once consolidation with DoITT has been completed, DoITT's Disaster Recovery plan, as it relates to DOE functionality, will be reviewed and approved by DOE management. As we consolidate with DoITT, we will also be developing disaster recovery plans along with our plans for server consolidation.

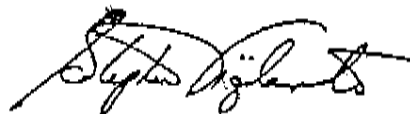
**TARGET IMPLEMENTATION DATE**

It is our intent to have mainframe computer disaster recovery completed by mid-February 2005 and a server disaster recovery plan in place by the end of calendar 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

Print Name:

Print Title: Deputy CIO/IT Operations

6/17/04

Date

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

- 4. Conduct a comprehensive test of the disaster recovery plan which should be followed by a similar test once a year, every year.

**RESPONSE TO RECOMMENDATION**

Once consolidation with DoITT is completed by the end of calendar 2004, the DOE will participate in all DoITT's Disaster Recovery tests which occur twice annually. As we consolidate with DoITT, we will also be developing disaster recovery plans along with our plans for server consolidation.

**TARGET IMPLEMENTATION DATE**

It is our intent to have mainframe computer disaster recovery completed by mid-February 2005 and a server disaster recovery plan in place by the end of calendar 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:   
Stephen Vigilante

6/17/04  
Date

Print Name: \_\_\_\_\_  
Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

5. Update the disaster recovery plan when the information it contains becomes obsolete.

**RESPONSE TO RECOMMENDATION**

We will update the existing disaster recovery plan and merge with DoITT's disaster recovery plan as it relates to DOE functionality once consolidation is complete with DoITT. DOE will be full participants in the testing of DoITT's Disaster Recovery program. DOE's disaster recovery plan will be further updated at the completion of the server consolidation.

**TARGET IMPLEMENTATION DATE**

It is our intent to have mainframe computer disaster recovery completed by mid-February 2005 and a server disaster recovery plan in place by the end of calendar 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

6. Establish and implement procedures for using polling software to catalog and monitor individual workstation hardware and software.

**RESPONSE TO RECOMMENDATION**

The DOE recognizes the benefits of this function and now has created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.

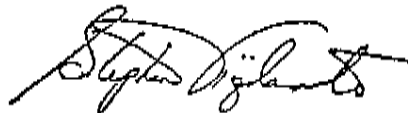
**TARGET IMPLEMENTATION DATE**

End of calendar year 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

7. Conduct regular penetration testing of its computer networks and document the results. In addition, DOE Internet Security should be updated, as needed, based on the result of the penetration testing.

**RESPONSE TO RECOMMENDATION**

The DOE recognizes the benefits of this function and now has created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.


**TARGET IMPLEMENTATION DATE**

End of calendar year 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations



NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**D. RECOMMENDATION WHICH THE AGENCY  
AGREES OR DISAGREES WITH AND WILL NOT IMPLEMENT (circle one)**

8. The DOE should establish and implement Internet security procedures for generating Web server statistics on all Web-related activities, including all Web sites accessed by the administrative staff.

**RESPONSE TO RECOMMENDATION  
(ALTERNATIVE SOLUTIONS ON CURRENT SITUATION CITED IN AUDIT REPORT)**

The DOE has over 130,000 administrative employees. To implement a plan to filter all administrative workstations would be cost prohibitive and difficult to monitor. The DOE maintains its policy of active supervision by administrative managers, directors, and supervisors.

**RESPONSIBILITY CENTER**

DIIT

Signature: 

Stephen Vigilante

6/17/04

Print Name: \_\_\_\_\_

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_\_ OF \_\_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

9. The DOE should establish and implement Internet security procedures for scanning all Web-related activity for unusual or suspicious activities.

**RESPONSE TO RECOMMENDATION**

The DOE recognizes the benefits of this function and now has created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.

**TARGET IMPLEMENTATION DATE**

Mid-calendar year 2005

**RESPONSIBILITY CENTER**

DIIT

Signature: 

Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**D. RECOMMENDATION WHICH THE AGENCY  
AGREES OR DISAGREES WITH AND WILL NOT IMPLEMENT (circle one)**

10. The DOE should establish and implement Internet security procedures for using filtering software to control access to undesirable Web sites by administrative staff.

**RESPONSE TO RECOMMENDATION  
(ALTERNATIVE SOLUTIONS ON CURRENT SITUATION CITED IN AUDIT REPORT)**

The DOE has over 130,000 administrative employees. To implement a plan to filter all administrative workstations would be cost prohibitive and difficult to monitor. The DOE maintains its policy of active supervision by administrative managers, directors, and supervisors.

**RESPONSIBILITY CENTER**

DIIT

Signature:



Stephen Vigilante

6/17/04

Print Name:

Date

Print Title:

Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**C. RECOMMENDATION WHICH THE AGENCY  
AGREES WITH BUT IS PENDING IMPLEMENTATION**

11. The DOE should establish and implement procedures for monitoring all inbound and outbound traffic passing through the firewalls.

**RESPONSE TO RECOMMENDATION**

The DOE recognizes the benefits of this function and now has created a security office with a manager charged with examining and strengthening our security procedures. As funding becomes available, we will implement procedures for advanced monitoring of our computer network.

**TARGET IMPLEMENTATION DATE**

End of calendar year 2005

**RESPONSIBILITY CENTER**

DIIT

Signature:   
Stephen Vigilante

6/17/04

Print Name:

Date

Print Title: Deputy CIO/IT Operations

NEW YORK CITY DEPARTMENT OF EDUCATION  
OFFICE OF AUDITOR GENERAL  
External Audit Services

PAGE \_\_\_ OF \_\_\_

RESPONSE DATE: June 17, 2004

AUDIT TITLE: Second Follow-up Audit Report on DOE Internal Controls Over Its Data Center

AUDITING AGENCY: Department of Education

DIVISION: Instructional and Information Technology

DRAFT REPORT DATE: June 9, 2004

AUDIT NUMBER: 7F04-137

**B. RECOMMENDATION WHICH THE AGENCY  
HAS PARTIALLY IMPLEMENTED**

12. DOE should ensure that it actively manages system passwords. In this regard, DOE should develop written password policies for its networks. These policies should require users to periodically change their passwords and include procedures for reviewing the status of inactive user-IDs and terminating them, as appropriate.

**WHAT HAS BEEN IMPLEMENTED?**

27 of the 98 IDs have been deleted from the list of IDs identified during the audit as being former employees. 21 of the 98 IDs are being reviewed and appear to be active consultants. 50 of the 98 IDs have been found to be active employees. Of the 6,635 IDs found to be duplicates, none are actually duplicates as the analysis appeared to compare only 4 characters of the ID whereas many IDs have more than 4 characters. We have begun to actively remove IDs for accounts not accessed for 120 days. We have also implemented a 90 day password change policy for Outlook e-mail accounts and have begun to develop written policies and procedures which will also be in effect for mainframe passwords.

**WHAT HAS TO BE IMPLEMENTED?**

We will continue to remove IDs for accounts that have not been accessed for 120 days. We will work with Human Resources to develop procedures for notification when an employee departs.

**EXPECTED IMPLEMENTATION DATE**

September 2004.

**RESPONSIBILITY CENTER**

DIIT

Signature:

  
Stephen Vicinanza

Print Name:

Print Title: Deputy CIO / OPERATIONS

6/17/2004  
Date