

AUDIT REPORT

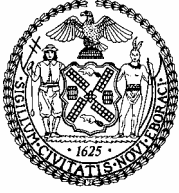


CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Second Follow-Up Audit Report on Data Processing Controls and Procedures of the Administration For Children's Services

7F05-083

May 19, 2005



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 14 recommendations made in a previous follow-up audit entitled, Follow-up Audit Report of the Data Processing Controls and Procedures of the Administration for Children's Services (Audit # 7F03-114, issued June 6, 2003).

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

Audits such as this provide a means of ensuring that City computer systems function reliably, contain accurate information, and are secure from unauthorized access.

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.

Very truly yours,

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

William C. Thompson, Jr.

WCT/gr

Report: 7F05-083
Filed: May 19, 2005

Table of Contents

AUDIT REPORT IN BRIEF	1
Audit Findings and Conclusions	1
Audit Recommendations	2
INTRODUCTION	3
Background	3
Objectives	3
Scope and Methodology	3
Discussion of Audit Results	4
RESULTS OF FOLLOW-UP AUDIT	5
ADDENDUM Administration for Children Services Response	

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

**Second Follow-Up Audit Report on
Data Processing Controls and Procedures of the
Administration for Children's Services**

7F05-083

AUDIT REPORT IN BRIEF

This second follow-up audit determined whether the Administration for Children's Services (ACS) implemented the 14 recommendations made in a previous follow-up audit of ACS' data processing controls. In this report, we discuss the 14 recommendations from the prior audit in detail, as well as the implementation status of each recommendation.

On June 6, 2003, our office conducted a follow-up audit to determine whether ACS implemented 18 recommendations contained in a previous audit of ACS' data processing controls and procedures, which was issued on January 9, 2001. The 2003 audit disclosed that ACS only implemented six of the 18 recommendations; three were partially implemented, and nine were not implemented. In addition, the audit disclosed new findings pertaining to weaknesses in access controls over the system. To address these issues, the 2003 report contained 14 recommendations, which included two recommendations to address the new findings.

Audit Findings and Conclusions

Despite assurances from ACS officials that corrective action would be taken to address the issues raised in our two prior audit reports (issued on January 9, 2001, and June 6, 2003), many deficiencies still exist. Such weaknesses, if not addressed, increase the risk of unauthorized system access, business disruptions, misuse of sensitive data, and misappropriation of expensive equipment. Of 14 recommendations made in the previous follow-up audit, this audit disclosed that ACS implemented five, partially implemented three, and did not implement six. The issues that have not been addressed include: implementing a disaster recovery plan; installing a fire suppression system at the Data Center; maintaining a complete and accurate record of computer hardware and software; ensuring that system passwords are periodically changed; deactivating user IDs of employees who are no longer

working for the agency; and, developing procedures for reviewing, investigating, and reporting failed login attempts.

To address these issues, this report recommends that ACS should:

- Implement the disaster recovery plan and conduct comprehensive tests of the plan, in accordance with Comptroller's Directive #18.
- Implement the Cisco Security Agent to reduce the risk of system intrusion.
- Ensure that the Data Center is equipped with an operating fire suppression system, in accordance with Directive 18.
- Develop a complete and accurate list of all of its computer equipment.
- Conduct annual inventory reconciliations and update its computer inventory list accordingly.
- Ensure that its inventory list of computer applications and software contains license numbers, number of licenses held, and names of users who are authorized to use each application.
- Conduct annual inventory reconciliations of all of its software licenses and update the inventory records accordingly.
- Ensure that passwords are changed at predetermined intervals.
- Ensure that user IDs are deactivated in accordance with its procedures.
- Develop and implement procedures for reviewing, investigating, and reporting failed remote logins, in accordance with Directive #18.

INTRODUCTION

Background

ACS provides protection to children subjected to abuse and neglect; preventive services to families to maintain the safety of children; and, when necessary, provides children with safe foster care or adoptive homes. Directly or through contracts, ACS also administers child care, early childhood education, and child support enforcement services.

Within ACS, the Office of Management Information Services (MIS) is responsible for purchasing computer equipment; developing and supporting application software; and operating the Data Center. The Data Center is the primary ACS data processing facility. The Data Center supports a vast computer network infrastructure that enables ACS to communicate with its own remote sites.

In June 2003, the Comptroller's Office issued a follow-up report to an audit it conducted in 2001 on ACS' data processing controls and procedures (7A00-151, issued January 9, 2001). That audit disclosed that ACS did not implement many of the 2001 audit recommendations—only six of the 18 recommendations were implemented, three were partially implemented, and nine were not implemented. Specifically, the 2003 audit concluded that ACS: did not ensure that users periodically change their network passwords; did not deactivate the accounts of inactive or former employees; allowed users unlimited login attempts from remote sites; did not monitor the activities of its domain administrators; did not have procedures to review, investigate and report failed remote logins; lacked a comprehensive disaster recovery plan; did not conduct and maintain an accurate inventory of computer equipment and software items; needed to improve their fire-prevention and fire-extinguishing controls; and lacked adequate change control procedures.

Objective

This follow-up audit determined whether ACS implemented the 14 recommendations contained in a previous audit, *Follow-up Audit of the City of New York's Administration for Children's Services Data Processing Controls and Procedures* (Audit No. 7F03-114, issued June 6, 2003).

Scope and Methodology

The time period reviewed in this audit was September 2004 through November 2004. To determine the implementation status of the recommendations, we:

- reviewed prior audit reports issued by the Comptroller's Office (*Audit of the City of New York's Administration for Children's Services Data Processing Controls and Procedures* - Audit #7A00-151, issued January 9, 2001; *Follow-up Audit Report on the Data Processing Controls and Procedures of the Administration for Children's Services* - Audit No. 7F03-114, issued June 6, 2003);

- reviewed and analyzed ACS disaster recovery documentation;
- reviewed and analyzed the ACS change control procedures;
- toured the Data Center to ascertain whether ACS implemented the physical and system security measures recommended in the previous audit;
- reviewed and analyzed the ACS computer equipment and software inventory;
- Tested the ACS user list to check whether the access to the network has been disabled for employees who left ACS during the CY 2003.

For the audit's criteria we used: 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; the United States General Accounting Office "Federal Information Systems Control Audit Manual," issued January 1999; 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.

Discussion of Audit Results

The matters covered in this report were discussed with ACS officials during and at the conclusion of this audit. A preliminary draft report was sent to ACS officials and discussed at an exit conference held on March 22, 2005. On April 5, 2005, we submitted a draft report to ACS officials with a request for comments. We received a written response from ACS officials on April 20, 2005 stating that they agreed with the audits recommendations.

The full text of the ACS response is included as an addendum to this report. However, for security reasons certain sensitive information contained in the ACS response (pertaining to the location of the agency's disaster recovery site) has been redacted.

RESULTS OF FOLLOW-UP AUDIT

Of 14 recommendations made in the previous follow-up audit, this audit disclosed that ACS implemented five, partially implemented three, and did not implement six. The issues that have not been addressed include: implementing a disaster recovery plan; installing a fire suppression system at the Data Center; maintaining a complete and accurate record of computer hardware and software; ensuring that system passwords are periodically changed; deactivating user IDs of employees who are no longer working for the agency; and, developing procedures for reviewing, investigating, and reporting failed remote login attempts.

Previous Finding: “ACS hired Veritas Software Corporation (Veritas) to develop and implement a disaster recovery plan. Veritas delivered a proposed plan to ACS on October 8, 2002. However, with the exception of backing-up its data applications, ACS has not put the plan into operation.” In addition, “since the plan has not been implemented, ACS has not been able to update the plan or perform an annual comprehensive test.”

Previous Recommendation #1: “ACS should implement the disaster recovery plan and update the plan on an as-needed basis. Once the plan is implemented ACS should conduct a comprehensive test of the plan and schedule annual tests, as required by Comptroller’s Directive #18.”

Previous ACS Response: “ACS MIS will conduct a detailed analysis to determine Backup requirements; Backup type; Backup site location; Equipment needed; and Staff requirements. A short-term purchase request will be submitted within the existing budget for required equipment and a long-term additional funding request will also be submitted for the required equipment. ACS MIS will develop short-term and long-term testing plans and procedures and backup/recovery equipment will be setup. ACS MIS will conduct comprehensive tests of the plan and schedule annual tests as required.”

Current Status: NOT IMPLEMENTED

ACS still has not implemented a disaster recovery plan for its systems. Therefore, we consider recommendation #1 not implemented.

Recommendation

1. ACS should implement a disaster recovery plan and conduct comprehensive tests of the plan, in accordance with Comptroller’s Directive #18.

ACS Response: “ACS/MIS has already begun to partially implement a disaster recovery plan. It has identified a site . . . as its disaster recovery storage site. ACS/MIS has also had a preliminary discussion with DoITT regarding data line redundancy between all ACS sites and the disaster recovery site as well as all

ACS sites and . . . William Street. The next step will be to develop a plan, which will outline the steps, schedules for milestones, and requirements for equipment. Options will be determined and funding will be requested.”

Previous Finding: “ACS . . . has formal program change policies. However, ACS . . . does not maintain a log of system changes.”

Previous Recommendation #2: “ACS should require that MIS personnel record all system changes in a log. The log should indicate what feature was modified and the reason for the modification.”

Previous ACS Response: “ACS MIS will implement a requirement for MIS personnel to log all system changes indicating what feature was modified and the reason for the modification.”

Current Status: IMPLEMENTED

ACS officials now maintain daily logs of all changes made to the system. The logs are reviewed by designated agency personnel. Accordingly, we consider recommendation #2 implemented.

Previous Finding: “The Callback function for the Cisco Secure remote access software, which requires the ACS Data Center computer to dial the user back, is not activated.”

Previous Recommendation #3: “ACS should activate the Callback function contained in the Cisco software.”

Previous ACS Response: “ACS MIS Management has deemed that the dual password combination currently employed is sufficient to address security concerns. In addition, the call back function has not been implemented since staff must travel to multiple locations and this function will not work due to its static nature.”

Current Status: PARTIALLY IMPLEMENTED

ACS still has not installed a callback function on its network. However, ACS is in the process of addressing this issue by implementing the Cisco Security Agent, which will protect the network from unauthorized access from remote locations. Accordingly, we consider recommendation #3 to be partially implemented.

Recommendation

2. ACS should implement the Cisco Security Agent to reduce risk of system intrusion.

ACS Response: “ACS/MIS has already begun to partially implement the Cisco Security Agent. ACS/MIS has begun testing this in 01/05. Currently, it is on 300 computers. By the end of May, coincident with the rollout of new computers, ACS/MIS will complete the installation of the Cisco Security Agent. ACS/MIS will introduce the Cisco Security Agent to all of its computers.”

Previous Finding: “ACS has not installed a smoke detection system, nor does it have an operating fire suppression system.”

Previous Recommendation #4: “ACS should install smoke detectors in the Data Center, both on the ceiling and under all raised floors, and train Data Center staff in locating and maintaining them.”

Previous ACS Response: “ACS MIS installed a fire alarm panel and smoke detection system with ceiling and under floor detectors, as well as under floor water detectors. The system includes break glass shunt-trip power shut down, fan shut down, and pull station and it is tied into the building fire alarm system, and thus into a Central Station Company, which contacts FDNY. The date for FDNY inspection and testing is pending. MIS staff training will follow.”

Current Status: IMPLEMENTED

ACS has installed smoke detectors on the ceiling and under all raised floors of the Data Center. The smoke detectors establish direct communication with Fire Department and building security in the event of a fire. Therefore, we consider recommendation #4 implemented.

Previous Recommendation #5: “ACS should ensure that the Data Center is equipped with an operating fire suppression system in accordance with Directive #18.

Previous ACS Response: “An electrical vendor has submitted a proposal to ACS Facilities for gas/fire suppression for the Data Center.”

Current Status: NOT IMPLEMENTED

ACS has not installed a fire suppression system at the data center. Therefore, we consider recommendation #5 not implemented.

Recommendation

3. ACS should ensure that the Data Center is equipped with an operating fire suppression system, in accordance with Directive 18.

ACS Response: “ACS has also begun to partially implement a fire suppression system. ACS facilities has been working to install the fire suppression system. It has upgraded the electricity in the data center, replaced the ceiling and floor with new and stronger tiles, which are leak proof and would prevent the gas from leaking to surrounding areas, upgraded the air conditioning, rewired the alarm system and expanded the room, all needed to accommodate the fire suppression system.

“Facilities has to install pipes in the ceiling, finish sealing of the ceiling and floors, install the under floor piping and specialized fire control wiring, replace all lights to avoid leakage, and add gas tanks.”

Previous Finding: “ACS . . . does not conduct annual inventory reconciliations of its computer equipment, nor does affix identification tags to the equipment.”

Previous Recommendation #6: “Conduct an annual inventory reconciliation of all its computer equipment.”

Previous ACS Response: “ACS MIS will conduct a baseline inventory of all desktop computer equipment in all of its sites. ACS MIS will enter baseline inventory data into Track IT! – the ACS MIS inventory management repository. ACS MIS will maintain and monitor inventory accuracy by capturing changes on the ACS MIS Asset Activity Tracking Sheet and assign a person responsible to conduct an annual inventory reconciliation of all computer equipment.”

Current Status: NOT IMPLEMENTED

ACS has not performed annual inventory reconciliations of its computer equipment, as recommended in the previous audit. Consequently, its current inventory list is incomplete; it does not include equipment such as printers, keyboards, servers, and network routers for all office sites. Therefore, we consider recommendation #6 not implemented.

Recommendations

4. Develop a complete and accurate list of all of its computer equipment.

ACS Response: “ACS/MIS has begun to partially implement this action. ACS/MIS has just updated its baseline inventory for its computers, printers, servers, and routers. Additionally, ACS/MIS has had in its possession the

inventory of all ACS printers, servers, and routers. These documents were provided to the Comptroller at the Exit Conference as an appendix.”

5. Conduct annual inventory reconciliations and update its computer inventory list accordingly.

ACS Response: “ACS has also begun to partially implement this action. ACS has just updated its inventory baseline. These documents were provided to the Comptroller at the Exit Conference as an appendix. ACS will conduct annual inventory reconciliation and update its computer inventory list accordingly.”

Previous Recommendation #7: “Affix identification tags to all of its computer equipment.”

Previous ACS Response: “ACS MIS will conduct research and planning, draft and finalize tag language design, and determine cost estimate for purchase request. ACS MIS will implement an affix of identification tags to all of ACS’ computer equipment.”

Current Status: IMPLEMENTED

We found that ACS has affixed identification tags to its equipment. Therefore, we consider recommendation #7 implemented.

Previous Finding: “Several software items installed on the agency’s system were not included on the list” of in-house computer applications and software that was supplied by ACS.

Previous Recommendation #8: “ACS should maintain an inventory list of computer applications and software indicating the number of licenses held for each software item.

Previous ACS Response: “ACS MIS will develop and initiate a plan to integrate application and software tracking databases to maintain an inventory of computer applications and software indicating the number of licenses held for each software item.”

Current Status: PARTIALLY IMPLEMENTED

ACS provided a list of its software inventory. However, the list is missing important information including license numbers and location of each application. Accordingly, we consider recommendation #8 partially implemented.

Recommendation

- 6. ACS should ensure that its inventory list of computer applications and software contains license numbers, number of licenses held, and names of users who are authorized to use each software application.

ACS Response: “ACS/MIS has implemented this action. The amended inventory includes the license numbers associated with the software previously inventoried and identifies the computers where the software is currently installed. These documents were provided to the Comptroller at the Exit Conference as an appendix.”

Previous Finding: “ACS . . . does not have inventory reconciliation procedures for its software licenses.”

Previous Recommendation #9: “ACS should conduct an annual inventory reconciliation of all of its software licenses.”

Previous ACS Response: “ACS MIS will develop and initiate a plan to evaluate and implement a software audit tool to conduct an annual inventory reconciliation of all of its software licenses.”

Current Status: NOT IMPLEMENTED

ACS has not performed annual inventory reconciliations of its computer applications and software licenses, as recommended. Accordingly, we consider recommendation #9 not implemented.

Recommendation

- 7. ACS should conduct annual inventory reconciliations of all of its software licenses and update the inventory records accordingly.

ACS Response: “ACS/MIS will do an annual inventory reconciliation of its baseline.”

Previous Finding: “ACS does not ensure that users periodically change their Cisco and NT passwords.”

Previous Recommendation #10: “ACS should ensure that passwords are changed at predetermined intervals.”

Previous ACS Response: “The feature to ensure that users are prompted to change their passwords every 90 days will be activated.”

Current Status: NOT IMPLEMENTED

ACS still does not ensure that users periodically change their Cisco and NT passwords. Accordingly, we consider recommendation #10 not implemented.

Recommendation

8. ACS should ensure that passwords are changed at predetermined intervals.

ACS Response: “ACS/MIS has begun to partially implement this action. ACS has instituted a procedure for all ACS employees to change their password twice a year.”

Previous Finding: “It [ACS] does not ensure that the accounts of terminated employees are deactivated.”

Previous Recommendation #11: “ACS should establish and implement formal procedures for deactivating system access of terminated employees.”

Previous ACS Response: “ACS MIS will institute a management review process of existing procedures for deactivating system access of terminated employees.”

Current Status: PARTIALLY IMPLEMENTED

ACS now has a procedure for deactivating user IDs of employees who are no longer employed by the agency. However, we noted that this procedure is not always followed. Specifically, ACS did not deactivate user IDs of 93 employees who were on leave, 12 who were terminated, and one who was suspended. Accordingly, we consider recommendation #11 only partially implemented.

Recommendation

9. ACS should ensure that user IDs are deactivated in accordance with its procedures.

ACS Response: “ACS/MIS also receives a list from Personnel of terminations and deactivates them. MIS and Personnel will work to establish a procedure for long-term leave and follow up on termination deactivations.”

Previous Finding: “It [ACS] allows users unlimited login attempts from remote sites.”

Previous Recommendation #12: “ACS should disconnect remote access of users after a specified number of failed login attempts.”

Previous ACS Response: “ACS MIS will activate the feature to disconnect remote access of users after three (3) login attempts.”

Current Status: IMPLEMENTED

ACS has activated the system feature that locks out remote users after three failed login attempts. Accordingly, we consider recommendation #12 implemented.

Previous Finding: “ACS does not monitor the activities of its 17 Domain Administrators.”

Previous Recommendation #13: “ACS should monitor the activities of users with Domain Administrator access in accordance with Directive #18.”

Previous ACS Response: “ACS MIS will institute a periodic management review process to monitor the activities of users with Domain Administrator access.”

Current Status: IMPLEMENTED

ACS now utilizes the Windows NT security audit feature to create a weekly log, which is used to monitor the activities of users with Domain Administrator access. Therefore, we consider recommendation #13 implemented.

Previous Finding: ACS generates “monthly reports of successful and failed remote logins. However, ACS has not developed procedures for reviewing these reports.”

Previous Recommendation #14: “ACS should develop and implement procedures for reviewing, investigating, and reporting failed remote logins, in accordance with Directive #18.”

Previous ACS Response: “The ACS MIS Security Office will review the system logs for failed remote logins every 30 days and will formally report findings to Network Services management.”

Current Status: NOT IMPLEMENTED

ACS still has not developed formal procedures for reviewing, investigating and reporting failed remote logins. Accordingly we consider recommendation #14 not implemented.

Recommendation

10. ACS should develop and implement procedures for reviewing, investigating and reporting failed remote logins, in accordance with Directive 18.

ACS Response: “ACS/MIS has implemented a formal procedure for reviewing, investigating, and reporting failed remote logins in accordance with Directive 18, and has submitted documentation to the Comptroller. MIS currently has a procedure in place to generate a log of failed remote logins. MIS has designated a person to monitor this report on a daily basis and send to the Manager of Network Operations.”



ADMINISTRATION FOR CHILDREN'S SERVICES
FINANCIAL SERVICES
150 William Street - 10th Floor
New York, NY 10038

JOHN B. MATTINGLY
Commissioner

SUSAN NUCCIO
Deputy Commissioner

April 18, 2005

Mr. Greg Brooks
Deputy Comptroller
Policy, Audits, Accountancy & Contracts
The City of New York Office of the Comptroller
Executive Offices
1 Centre Street, Room 1100
New York, New York 10007-2341

Re: NYC Comptroller's Second Follow-Up Audit Report 7F05-083 on
Data Processing Controls and Procedures of the
Administration for Children's Services

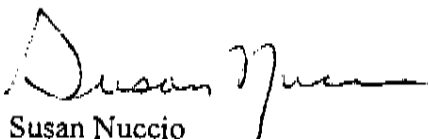
Dear Mr. Brooks:

Thank you for sharing with us the Draft Report for the above captioned audit.

Attached is our response to your recommendations and appropriate Audit Implementation Plans (AIPs). ACS looks forward to working with your office to improve the delivery of services to the children of the City of New York.

If you have any questions, please do not hesitate to contact me.

Sincerely,


Susan Nuccio

Attachments

City of New York Office of the Comptroller
Second Follow-Up Audit Report on Data Processing Controls and
Procedures of the Administration for Children's Services
Audit Number 7F05-083

Administration for Children's Services (ACS)
Response to Recommendations
April 13, 2005

Recommendations 1 and 3

ACS/MIS has already begun to partially implement a disaster recovery plan. It has identified a site at [REDACTED] Street as its disaster recovery storage site. ACS/MIS has also had a preliminary discussion with DOITT regarding data line redundancy between all ACS sites and the disaster recovery site as well as all ACS sites and 150 William Street. The next step will be to develop a plan, which will outline the steps, schedules for milestones, and requirements for equipment. Options will be determined and funding will be requested.

ACS/MIS has also begun to partially implement a fire suppression system. ACS Facilities has been working to install the fire suppression system. It has upgraded the electricity in the data center, replaced the ceiling and floor with new and stronger tiles, which are leak proof and would prevent the gas from leaking to surrounding areas, upgraded the air conditioning, rewired the alarm system and expanded the room, all needed to accommodate the fire suppression system.

Facilities has to install pipes in the ceiling, finish sealing of the ceiling and floors, install the under floor piping and specialized fire control wiring, replace all lights to avoid leakage, and add gas tanks.

Recommendation 2

ACS/MIS has already begun to partially implement the Cisco Security Agent. ACS/MIS has begun testing this in 01/05. Currently, it is on 300 computers. By the end of May, coincident with the rollout of new computers, ACS/MIS will complete the installation of the Cisco Security Agent. ACS will introduce the Cisco Security Agent to all of its computers.

Recommendations 4 and 5

ACS/MIS has begun to partially implement this action. ACS/MIS has just updated its inventory baseline for its computers, printers, servers, and routers. Additionally ACS/MIS has had in its possession the inventory of all ACS printers, servers and routers. These documents were provided to the Comptroller at the Exit Conference as an appendix.

ACS/MIS has also begun to partially implement this action. ACS has just updated its inventory baseline. These documents were provided to the Comptroller at the Exit Conference as an appendix. ACS will conduct annual inventory reconciliations and update its computer inventory list accordingly.

Recommendations 6 and 7

ACS/MIS has implemented this action. The amended inventory includes the license numbers associated with the software previously inventoried and identifies the computers where the software is currently installed. These documents were provided to the Comptroller at the Exit Conference as an appendix. ACS/MIS will do an annual inventory reconciliation of its baseline.

Recommendations 8, 9, and 10

ACS/MIS has begun to partially implement this action. ACS has instituted a procedure for all ACS employees to change their password twice a year. ACS/MIS also receives a list from Personnel of terminations and deactivates them. MIS and Personnel will work to establish a procedure for long-term leave and follow up on termination deactivations.

ACS/MIS has implemented a formal procedure for reviewing, investigating, and reporting failed remote logins in accordance with Directive 18 and has submitted documentation to the Comptroller. MIS currently has a procedure in place to generate a log of failed remote logins. MIS has designated a person to monitor this report on a daily basis and send to the Manager of Network Operations.

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 1: ACS should implement the disaster recovery plan and conduct comprehensive tests of the plan, in accordance with Comptroller's Directive #18.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has begun to partially implement this action. It has identified a site at [REDACTED] as its disaster recovery storage site. MIS also had a preliminary discussion with DOTT regarding data line redundancy between all ACS sites and the disaster recovery site as well as all ACS sites and [REDACTED].</p> <p>The next step will be to develop a plan, which will outline the steps, schedules for milestones, and requirements for equipment. Options will be determined and funding will be requested.</p>	<p>Aryeh Norensberg, Assistant Commissioner Network and Operation Services</p>	<p>03/05</p>	<p>05/05</p>		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 2: ACS should implement the Cisco Security Agent to reduce risk of system intrusion.
RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has begun to partially implement this action. ACS/MIS has begun testing this in 01/05. Currently, it is on 300 computers. By the end of 05/05, coincident with the rollout of new computers, ACS/MIS will complete the installation of the Cisco Security Agent.</p> <p>ACS/MIS will introduce the Cisco Security Agent to all of its computers.</p>	<p>Aryeh Norensberg, Assistant Commissioner Network and Operation Services</p>	<p>01/05</p>	<p>06/05</p>		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 3: ACS should ensure that the Data Center is equipped with an operating fire suppression system, in accordance with Directive 18.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has begun to partially implement this action. ACS Facilities has been working to install the fire suppression system. It has upgraded the electricity in the data center, replaced the ceiling and floor with new and stronger tiles, which are leak proof and would prevent the gas from leaking to surrounding areas, upgraded the air conditioning, rewired the alarm system and expanded the room, all needed to accommodate the fire suppression system.</p> <p>Facilities has to install pipes in the ceiling, finish sealing of the ceiling and floors, install the under floor piping and specialized fire control wiring, replace all lights to avoid leakage, and add gas tanks.</p>	<p>Mich Edwards, Supervisor of Mechanics (SOM) And Arveh Norensberg, Assistant Commissioner Network and Operation Services</p>	<p>12/04</p>	<p>06/05</p>		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 4: ACS should develop a complete and accurate list of all of its computer equipment.
RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has begun to partially implement this action. ACS/MIS has just updated its inventory baseline for its computers, printers, servers, and routers. Additionally ACS/MIS has had in its possession the inventory of all ACS printers, servers and routers. These documents were provided to the Comptroller at the Exit Conference as an appendix.</p>	<p>Stephen Feger, Director of Asset Management and Aryeh Norensberg, Assistant Commissioner Network and Operation Services</p>	<p>Completed</p>			

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 5: ACS should conduct annual inventory reconciliations and update its computer inventory list accordingly.
RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
ACS/MIS has begun to partially implement this action. ACS/MIS has just updated its inventory baseline. These documents were provided to the Comptroller at the Exit Conference as an appendix. ACS/MIS will conduct annual inventory reconciliations and update its computer inventory list accordingly.	Stephen Feger, Director of Asset Management	07/01/05	07/15/05		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 6: ACS should ensure that its inventory list of computer applications and software contains license numbers, number of licenses held, and names of users who are authorized to use each software application.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START END		DOCUMENTATION	COMMENTS
<p>ACS/MIS has implemented this action. The amended inventory includes the license numbers associated with the software previously inventoried and identifies the computers where the software is currently installed.</p> <p>These documents were provided to the Comptroller at the Exit Conference as an appendix.</p>	<p>Stephen Feger, Director of Asset Management</p>	<p>Completed</p>			

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 7: ACS should conduct annual inventory reconciliations of all of its software licenses and update the inventory records accordingly.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
ACS/MIS has begun to partially implement this action. ACS/MIS will do an annual inventory reconciliation of its baseline.	Stephen Feger, Director of Asset Management	09/12/05	09/19/05		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7P05-083**

RECOMMENDATION # 8: ACS should ensure that passwords are changed at predetermined intervals.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
ACS/MIS has begun to partially implement this action. ACS/MIS has instituted a procedure for all ACS employees to change their password twice a year.	Aryeh Norensberg, Assistant Commissioner Network and Operation Services	07/01/05	Continuing		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION #9: ACS should ensure that user IDs are deactivated in accordance with its procedures.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has begun to partially implement this action. ACS/MIS receives a list from Personnel of terminations and deactivates them. ACS/MIS and Personnel will work to establish a procedure for long-term leave and follow up on termination deactivations.</p>	<p>Arveh Norensberg, Assistant Commissioner Network and Operation Services and Janet Subrizi, Assistant Commissioner Personnel</p>	<p>06/01/05</p>	<p>Continuing</p>		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S SECOND FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F05-083**

RECOMMENDATION # 10: ACS should develop and implement formal procedures for reviewing, investigating and reporting failed remote logins, in accordance with Directive 18.

RESPONSIBLE MANAGER'S NAME: Dan Sedlis, Associate Commissioner, ACS/MIS

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	DOCUMENTATION	COMMENTS
<p>ACS/MIS has implemented this action and has submitted documentation to the Comptroller.</p> <p>MIS currently has a procedure in place to generate a log of failed remote logins. MIS has designated a person to monitor this report on a daily basis and send to the Manager of Network Operations.</p>	<p>Argyel Norensberg, Assistant Commissioner Network and Operation Services</p>	<p>Completed</p>			