AUDIT REPORT

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

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

7F03-114

June 6, 2003

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

June 6, 2003

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the Comptroller's responsibilities contained in Chapter 5, § 93, of the New York City Charter, my office has performed a follow-up audit that determined whether the New York City Administration for Children's Services (ACS) implemented recommendations made in a previous audit entitled, *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). The results of our audit, which are presented in this report, have been discussed with officials from New York City Administration for Children's Services, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that City agencies have appropriate policies and procedures to manage and safeguard their automated information systems and data processing resources.

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,

William C. Thompson Jr

William C. Thompson, Jr.

WCT/GR

Report: **7F03-114**
Filed: **June 6, 2003**

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

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

7F03-114

SUMMARY OF FOLLOW-UP FINDINGS

This follow-up audit determined whether the New York City Administration for Children's Services (ACS) implemented recommendations made in a previous audit entitled, *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). The earlier audit determined the adequacy of the Data Center's disaster recovery plans, program change control procedures, data security procedures, physical security procedures, and operational procedures for protecting ACS computer assets and information; the agency's compliance with the Comptroller's Internal Control and Accountability Directive #18, "Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems." In this current audit, we discuss the recommendations we made earlier, as well as the implementation status of those recommendations. We also discuss new findings and recommendations based on our current review.

In the previous audit, we made 18 recommendations to ACS, of which six have been implemented, three have been partially implemented, and nine have not been implemented. The details of these recommendations and their implementation follow.

1. "ACS MIS [Office of Management Information Services] should develop and implement a disaster recovery plan that is in full compliance with Comptroller's Directive #18. This would include maintaining an off-site location for storing backup data." **PARTIALLY IMPLEMENTED**

2. "ACS MIS should update the plan on an as-needed basis, as required by Comptroller's Directive #18." **NOT IMPLEMENTED**

3. "ACS MIS should conduct a comprehensive test of the plan on an annual basis, as required by Comptroller's Directive #18." **NOT IMPLEMENTED**

4. “ACS MIS should create a formalized change control program that fully meets the standards of Comptroller’s Directive #18 and the GAO Federal Information Systems Controls Audit Manual.” **PARTIALLY IMPLEMENTED**

5. “ACS MIS should develop security procedures that ensure that non-ACS Cisco Secure users who resign, or are terminated, from their agency have their privileges immediately revoked when such changes in employment occur.” **IMPLEMENTED**

6. “Data security staff should set proper security features for remote dial-in users (i.e., activate the Callback function, restrict time of access, etc.).” **NOT IMPLEMENTED**

7. “ACS MIS should issue network security control reports. Those reports should be generated by the systems security staff on a regular basis and should include such security violations as unsuccessful attempts to remotely access ACS computer networks, the passwords used in those attempts, and the times of access and times of attempts to access the ACS networks.” **IMPLEMENTED**

8. “ACS MIS should review all the ACS Enterprise network accounts with special privileges, determine the number of accounts that can be removed, and remove those accounts.” **IMPLEMENTED**

9. “ACS MIS should establish fire safety and fire control procedures. All staff members should be trained in following such procedures.” **IMPLEMENTED**

10. “ACS MIS should install smoke detectors in the Data Center, both on the ceiling and under all raised floors, and should train the staff in locating and maintaining them.” **NOT IMPLEMENTED**

11. “ACS MIS should install a system that will determine when a smoke detector is activated, and notify appropriate emergency personnel.” **NOT IMPLEMENTED**

12. “ACS MIS should periodically test all fire extinguishing equipment and smoke detectors in the Data Center for readiness in case of fire.” **NOT IMPLEMENTED**

13. “ACS should secure the Data Center room against environmental risks. A possible solution, short of relocating the Data Center to a new and safer location, would be to wall in the windows of the Data Center room.” **IMPLEMENTED**

14. "ACS MIS should use formal property pass procedures to keep track of, and ensure that, the removal of ACS MIS property (equipment, tapes, and supplies) is properly authorized, tracked, and accounted for." **IMPLEMENTED**

15. "ACS should conduct annual inventory reconciliation procedures for all computer equipment it uses." **NOT IMPLEMENTED**

16. "ACS should establish an individual property identification tag for each unit of computer equipment it owns." **NOT IMPLEMENTED**

17. "ACS should identify and maintain an inventory of the automated systems and software products that support each business function, including the numbers and types of software licenses in use." **PARTIALLY IMPLEMENTED**

18. "ACS should conduct annual inventory reconciliation procedures for all software licenses it uses." **NOT IMPLEMENTED**

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

1. Implement the disaster recovery plan and update the plan on an as-needed basis. Once the plan is implemented, conduct a comprehensive test of the plan and schedule annual tests, as required by Comptroller's Directive #18.

2. 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.

3. Activate the callback function contained in the Cisco software.

4. 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.

5. Ensure that the Data Center is equipped with an operating fire suppression system, in accordance with Directive 18.

6. Conduct an annual inventory reconciliation of all computer equipment.

7. Affix identification tags to all of its computer equipment.

8. Maintain an inventory list of computer applications and software indicating the number of licenses held for each software item.

9. Conduct an annual inventory reconciliation of all of its software licenses.

SUMMARY OF NEW FINDINGS AND RECOMMENDATIONS

ACS does not ensure that users periodically change their Cisco and Microsoft Windows NT passwords and that the accounts of terminated employees are deactivated. ACS also allows users unlimited login attempts from remote sites. In addition, ACS does not monitor the activities of its 17 Domain Administrators who have access to the most critical network functions and data. Finally, although ACS generates monthly reports of successful and failed remote logins, it has not developed procedures for reviewing these reports.

To address these new issues, we recommend that ACS should:

10. Ensure that passwords are changed at predetermined intervals.

11. Establish and implement formal procedures for deactivating system access of terminated employees.

12. Disconnect remote access of users after a specified number of failed login attempts.

13. Monitor the activities of users with Domain Administrator access in accordance with Directive 18.

14. Develop and implement procedures for reviewing, investigating, and reporting failed remote logins, in accordance with Directive 18.

ACS Response

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 April 29, 2003. On April 30, 2003, we submitted a draft report to ACS officials with a request for comments. We received a written response from ACS on May 19, 2003.

In its response, ACS agreed to implement 13 of the report’s 14 recommendations. ACS did not agree to implement our recommendation to activate the call back function contained in the Cisco software. In that regard, ACS stated that “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.”

The full text of the ACS’ comments is included as an addendum to this report.

INTRODUCTION

Background

The Administration for Children's Services provides protection to children subjected to abuse and neglect; provides 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 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. Its data resides on Personal Computer file-servers made by the IBM Corporation, SUN Microsystems, Compaq Corporation, and CSS Lab Inc. The file-servers process information using the following operating systems: Microsoft Windows NT (NT), SUN Microsystems SOLARIS, Hewlett Packard UNIX, and IBM Corporation DOS. Some of the computerized database applications are Informix, Dbase III, FoxPro, Oracle, and SQL Server. Programming languages include Visual Basic, Java, C/C+, and the Microsoft Office Suite. The Data Center supports a vast computer network infrastructure that enables ACS to communicate with its own remote sites via dedicated T1 lines.

Objectives, Scope, and Methodology

This follow-up audit determined whether ACS implemented the 18 recommendations contained in a previous audit, *Audit of the City of New York's Administration for Children's Services Data Processing Controls and Procedures* (Audit No. 7A00-151, issued January 9, 2001).

Audit fieldwork began in October 2002 and ended in March 2003. To meet our objectives, we:

- reviewed and analyzed ACS disaster recovery documentation;
- reviewed and analyzed the ACS change control program procedures;
- reviewed and analyzed the security procedures for ACS network data, remote dial-in-access, assigning passwords, and accessing the Local Area Network (LAN);
- toured the Data Center to ascertain whether ACS implemented the physical and system security measures recommended in the previous audit;
- reviewed and analyzed ACS equipment and software inventory procedures;

- determined whether the Department of Investigations approved the ACS Internet Security Architecture Plan; and

- tested whether the access to the network has been disabled for a sample of 44 of 847 employees who left ACS during the period April–November 2002.

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 April 29, 2003. On April 30, 2003, we submitted a draft report to ACS officials with a request for comments. We received a written response from ACS on May 19, 2003.

In its response, ACS agreed to implement 13 of the report's 14 recommendations. ACS did not agree to implement our recommendation to activate the call back function contained in the Cisco software. In that regard, ACS stated that "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."

The full text of the ACS' comments is included as an addendum to this report.

FOLLOW-UP RESULTS AND RECOMMENDATIONS

PREVIOUS FINDING: "There is no Disaster Recovery Plan"

Previous Recommendation #1: "ACS MIS should develop and implement a disaster recovery plan that is in full compliance with Comptroller's Directive #18. This would include maintaining an off-site location for storing backup data."

Previous Recommendation #2: "ACS MIS should update the plan on an as-needed basis, as required by Comptroller's Directive #18."

Previous Recommendation #3: "ACS MIS should conduct a comprehensive test of the plan on an annual basis, as required by Comptroller's Directive #18."

Previous ACS Responses to #1, #2, and #3: "ACS MIS concurs with this finding and agrees with recommendations #1, #2 and #3. A solicitation will be prepared to procure a vendor to assist with developing an ACS MIS specific disaster recovery plan to include: a comprehensive test plan; procedures for plan update and maintenance; a procedure for maintaining offsite storage of tapes; and a plan for data center continuity."

Current Status: PARTIALLY IMPLEMENTED/NOT IMPLEMENTED

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 and applications, ACS has not put the plan into operation. We therefore consider Recommendation 1 partially implemented. Since the plan has not been implemented, ACS has not been able to update the plan or perform an annual comprehensive test. Therefore, we consider Recommendations #2 and #3 not implemented.

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.

Agency 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."

****

PREVIOUS FINDING: "There are no change control program policies or procedures in place."

Previous Recommendation #4: "ACS MIS should create a formalized change control program that fully meets the standards of Comptroller's Directive #18 and the GAO Federal Information System Controls Audit Manual."

Previous ACS Response: "ACS MIS recognizes that a more formal change control program is needed to better ensure quality assurance testing of application and operating system changes. ACS MIS is in the process of identifying resources to develop improved change control policies and procedures that include hiring a project director that will be responsible for change control program implementation."

Current Status: PARTIALLY IMPLEMENTED

ACS now has formal program change control policies. However, ACS still does not maintain a log of system changes, a key element of Directive 18 that states, "Key control principles include . . . fully documenting the modification process including the identification of the exact feature being modified or implemented." Accordingly, we consider Recommendation #4 partially implemented.

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.

Agency 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."

****

PREVIOUS FINDING: ACS does not have security procedures in place to ensure that non-ACS Cisco Secure users who resign, or are terminated, from the agency have their system privileges immediately revoked.

Previous Recommendation #5: "ACS MIS should develop security procedures that ensure that non-ACS Cisco Secure users who resign, or are terminated, from their agency have their privileges immediately revoked when such changes in employment occur."

Previous ACS Response: "ACS MIS' current process is that once MIS is notified of a person leaving the agency, MIS immediately removes that person's access from the system, and also stops dial-in and desktop access. When MIS is made aware of this information, current MIS procedures provide for quickly removing that person's privileges. MIS reviews the list of persons with dial-in access to confirm user authorization."

Current Status : IMPLEMENTED

ACS now has security procedures in place to ensure that system privileges are immediately revoked when non-ACS Cisco Secure users resign or are terminated from the agency. Accordingly, we consider Recommendation #5 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. Neither is the Time of Access feature, which allows users to dial in only at certain times of the day. Therefore, people could dial in after business hours, when there is less of a chance of being detected."

Previous Recommendation #6: "Data Security staff should set proper security features for remote dial-in users (i.e. activate the Callback function, restrict time of access, etc)."

Previous ACS Response: "ACS MIS currently permits 24 hours a day, 7 days a week dial in access due to the business needs for ACS to function 24 hours a day."

Current Status: NOT IMPLEMENTED

We accept ACS' position regarding the need to provide dial-up access to its system 24-hours a day, seven-days a week. However, ACS still has not activated the Callback function contained in the Cisco software. Accordingly, we consider Recommendation #6 not implemented.

Recommendation

3. ACS should activate the Callback function contained in the Cisco software.

Agency 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."

Auditor Comment: We agree that the call back feature would not work for those employees who travel to various field locations. However, this function could be activated for those employees who use dial-up access to work from borough offices and from their homes. Therefore, we reiterate our recommendation.

****

PREVIOUS FINDING: "The Cisco Secure Audit function, which monitors user activity, is not activated and security-violations reports were not generated. With the Cisco Secure Audit function not activated, an unauthorized intruder, once inside the various ACS networks, would be difficult to detect."

Previous Recommendation #7: "ACS MIS should issue network security control reports. Those reports should be generated by the systems security staff on a regular basis and should include such security violations as unsuccessful attempts to remotely access ACS computer networks, the passwords used in those attempts, and the times of access and times of attempts to access the ACS networks."

Previous ACS Response: "The ACS MIS Network Security group issues and reviews Network Security Control Reports on a weekly basis and investigates all attempts by any user to log in without proper authentication. Due to current staffing deficiencies, MIS is not in a position to conduct these reviews more often. It is ACS MIS' plan to increase staff in this area to provide for more frequent monitoring of these reports."

Current Status: IMPLEMENTED

MIS now issues monthly reports of successful and failed remote logins. Accordingly, we consider Recommendation #7 implemented.

****

PREVIOUS FINDING: "Seventeen users have access to the most critical network functions and data. Having that many people with this type of control over the computer networks presents a potential security risk."

Previous Recommendation #8: "ACS MIS should review all the ACS Enterprise network accounts with special privileges, determine the number of accounts that can be removed, and remove those accounts."

Previous ACS Response: "MIS has staff with high permission levels in order for them to be able to perform their jobs. . . . To reduce this number to a lower level, would compromise our ability to service over 2000 users of the ACS network, in a timely fashion. MIS must maintain a sufficient staff, that is determined by the need, to provide effective service levels to the users of our organization."

Current Status: IMPLEMENTED

Based on written justification provided by ACS, we agree that each of the 17 users require special system privileges to perform their job responsibilities. Accordingly, we consider Recommendation #8 implemented.

****

<u>PREVIOUS FINDING</u>: "ACS's fire-prevention and fire-extinguishing controls need to be improved."

> ***<u>Previous Recommendation #9</u>:*** "ACS MIS should establish fire safety and fire control procedures. All staff members should be trained in following such procedures."
>
> ***<u>Previous Recommendation #10</u>:*** "ACS MIS should install smoke detectors in the Data Center, both on the ceiling and under all raised floors, and should train the staff in locating and maintaining them."
>
> ***<u>Previous Recommendation #11</u>:*** "ACS MIS should install a system that will determine when a smoke detector is activated, and notify appropriate emergency personnel."
>
> ***<u>Previous Recommendation #12</u>:*** "ACS MIS should periodically test all fire extinguishing equipment and smoke detectors in the Data Center for readiness in case of fire."
>
> ***<u>Previous ACS Responses to #9, #10, #11, and #12</u>:*** "The ACS Computer Data Center has Fire Extinguishers and a Sprinkler system. Staff will be trained on the use of the fire extinguishing equipment and will be retrained on their duties as Fire Wardens and Deputy Wardens exclusively for the Computer Data Center. The newly trained staff will be separate and apart from the fire evacuation team established for that floor. A plan for periodic testing of this equipment for readiness will also be developed and executed.
>
> "The ACS Facilities Division plans to work with the building landlord to install smoke detectors in the ACS Computer Data Center, both in the ceiling and under the raised floor, which will be connected to the existing centralized fire alarm system. The building Fire Safety Director and Deputy Fire Safety Directors will monitor and maintain them. Staff will be made aware of their locations, and will also be instructed to contact the Fire Safety Directors if any irregularities are observed. Once the smoke detectors are installed, periodic testing for readiness will occur."

<u>Current Status</u>: IMPLEMENTED/NOT IMPLEMENTED

Fire safety and fire control procedures have been included in the ACS "Tenant Handbook." Accordingly, we consider Recommendation #9 implemented. However, ACS has not installed a smoke detection system, nor does it have an operating fire suppression system. Therefore, we consider Recommendations #10, #11, and #12 not implemented.

Recommendation

ACS should:

4. 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.

Agency 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."

5. Ensure that the Data Center is equipped with an operating fire suppression system in accordance with Directive #18.

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

****

PREVIOUS FINDING: "ACS's data center assets are at risk in event of catastrophic weather-related events."

Previous Recommendation #13: "ACS MIS should secure the Data Center room against environmental risks. A possible solution, short of relocating the Data Center to a new and safer location, would be to wall in the windows of the Data Center room."

Previous ACS Response: "ACS MIS concurs with this finding and agrees with recommendation 13. Most of the windows are blocked by air-conditioning equipment placed in the windows. Additionally, the glass is of a strong type that is not likely to shatter. However, ACS MIS will investigate the provision of a ¼ inch Plexiglas covering over the existing windows and other possible alternatives to secure the Data Center room against environmental risks. Moving the Data Center to an internal non-windowed area is less likely due to cost and space considerations"

Current Status: IMPLEMENTED

Plexiglas has been installed over the windows at the Data Center. Accordingly, we consider Recommendation #13 implemented.

****

PREVIOUS FINDING: **"**ACS' Data center property pass procedures need improvement."

Previous Recommendation #14: "ACS MIS should use a formal property pass procedure to keep track of, and ensure that, the removal of ACS MIS property (equipment, tapes, and supplies) is properly authorized, tracked, and accounted for."

Previous ACS Response: "ACS MIS and ACS Facilities will work together to review and improve the current property pass procedures that will incorporate checks on both the 12th Floor and the Lobby."

Current Status #14: IMPLEMENTED

Building pass procedures have been included in the ACS "Tenant Handbook." Accordingly, we consider Recommendation #14 implemented.

****

PREVIOUS FINDING: "ACS does not have a periodic inventory reconciliation of all computer equipment it acquired and is responsible for; and, there are no property identification tags."

Previous Recommendation #15: "ACS should conduct annual inventory reconciliation procedures for all computer equipment it uses."

Previous Recommendation #16: "ACS should establish an individual property identification tag for each unit of computer equipment it owns."

Previous ACS Responses to #15 and #16: "ACS MIS recognizes the need to better manage and move towards a perpetual inventory control process which includes: annual reconciliation procedures; formal log of deliveries; individual property ID tags; equipment inventory including software licenses and annual software license reconciliation. MIS plans to review and initiate improvements to MIS' current process which will include implementing a more robust inventory control software to facilitate these efforts."

Current Status: NOT IMPLEMENTED

ACS still does not conduct annual inventory reconciliations of its computer equipment, nor does it affix identification tags to the equipment. In September 2002, ACS provided "baseline inventories" of its computer equipment. However, these inventories do not satisfy the recommendation since they: do not cover all ACS sites; do not include serial numbers for all equipment items; and represent results of inventories conducted on varying days making it possible for items at some sites to be counted more than once. Accordingly, we consider Recommendations #15 and #16 not implemented.

Recommendations

ACS should:

6. Conduct an annual inventory reconciliation of all its computer equipment.

Agency 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."

7. Affix identification tags to all of its computer equipment.

Agency 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."

****

PREVIOUS FINDING: "ACS does not maintain an inventory listing of all software licenses it has purchased. MIS management was unable to reconcile the number of software licenses in use on the ACS computer network with the actual number of software licenses purchased. MIS management was unable to provide us with the specific number and types of the software packages owned and in use."

Previous Recommendation #17: "ACS should identify and maintain an inventory of the automated systems and software products that support each business function, including the numbers and types of software licenses in use."

Previous Recommendation #18: "ACS should conduct annual inventory reconciliation procedures for all software licenses it uses."

Previous ACS Responses to #17 and #18: "ACS MIS recognizes the need to better manage and move towards a perpetual inventory control process which includes: annual reconciliation procedures; formal log of deliveries; individual property ID tags; equipment inventory including software licenses and annual software license reconciliation. MIS plans to review and initiate improvements to MIS' current process which will include implementing a more robust inventory control software to facilitate these efforts."

Current Status: PARTIALLY IMPLEMENTED/NOT IMPLEMENTED

ACS provided a list of in-house computer applications and software used by the agency. However, several software items installed on the agency's system were not included on the list. Accordingly, we consider Recommendation #17 partially implemented. ACS still does not have inventory reconciliation procedures for its software licenses. Accordingly, we consider Recommendation #18 not implemented.

Recommendations

ACS should:

8. Maintain an inventory list of computer applications and software indicating the number of licenses held for each software item.

Agency 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."

9. Conduct an annual inventory reconciliation of all of its software licenses.

Agency 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."

NEW FINDINGS AND RECOMMENDATIONS

Access Controls Weaknesses

ACS does not ensure that users periodically change their Cisco and NT passwords; it does not ensure that the accounts of terminated employees are deactivated; and it allows users unlimited login attempts from remote sites.

Passwords control the applications or system information an individual is permitted to access. Access authorization must be carefully designed to insure that employees have access only to files or programs that are necessary for them to perform their jobs. When passwords are not changed regularly, it increases the opportunity unauthorized individuals to learn the passwords and use them to gain access to the network. Comptroller's Directive #18, § 8.1.2 (1), states, "Active password management includes: insuring that users are forced to change passwords periodically . . . . and deactivation of . . . accounts for employees whose services have terminated." We found five terminated employees who continued to have system access in our review of records for a sample of 44 terminated employees. One of these five employees still had access more than one year after termination.

Allowing unlimited numbers of login attempts gives hackers and unauthorized users greater opportunity to decipher the password. Comptroller's Directive #18, § 8.6, states, "Hackers may attempt to gain access through the trial of common or vendor supplied passwords, use of speed-dial configurations or the interception of passwords/access codes retrieved from Internet 'sniffers' or public dial-in systems. The risks associated with computer hacking include: (1) the disclosure of confidential organization data, (2) the destruction or alteration of critical organizational data, (3) the introduction of a virus or work into the network."

Users with Domain Administrator Level Access Not Monitored

ACS does not monitor the activities of its 17 Domain Administrators. As stated earlier, these individuals have access to the most critical network functions and data. Comptroller's Directive #18, § 6.3(1), states, "Individuals who have access to sensitive information resources should be subject to special security procedures."

Review of Network Security Control Reports Not Formalized

As mentioned earlier, ACS implemented the prior audit's recommendation to generate monthly reports of successful and failed remote logins. However, ACS has not developed procedures for reviewing these reports. Comptroller's Directive #18, § 11.5, states: "A record of the physical and logical security violations detected by software controls and other monitoring procedures must be reported to senior management. The most serious security violations should be reported to executive management. A review of security violations will highlight unresolved problems or weaknesses in internal controls and may show patterns of failure and abuse requiring remedial action."

Recommendations

ACS should:

10. Ensure that passwords are changed at predetermined intervals.

Agency Response: "The feature to ensure that users are prompted to change their passwords every 90 days will be activated."

11. Establish and implement formal procedures for deactivating system access of terminated employees.

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

12. Disconnect remote access of users after a specific number of failed login attempts.

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

13. Monitor the activities of users with Domain Administrator access, in accordance with Directive #18.

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

14. Develop and implement procedures for reviewing, investigating, and reporting failed remote logins, in accordance with Directive #18.

Agency 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."

Administration for Children's Services

150 William Street – 18th Floor
New York, New York 10038

William C. Bell
Commissioner

May 19, 2003

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 Follow-Up Audit Report 7F03-114 on the 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,

Will C Bell

William C. Bell

Attachments

City of New York Office of the Comptroller
Follow-Up Audit Report on Data Processing and
Procedures of the Administration for Children's Services
Audit Number 7F03-114

Administration for Children's Services (ACS)
Response to Recommendations
May 19, 2003

Recommendation 1

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.

Recommendation 2

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.

Recommendations 3, 10, and 13

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. The feature to ensure that users are prompted to change their passwords every 90 days will be activated. ACS MIS will institute a periodic management review process to monitor the activities of users with Domain Administrator access.

Recommendations 4 and 5

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. An electrical vendor has submitted a proposal to ACS Facilities for gas/fire suppression for the Data Center.

Recommendations 6, 7, 8, and 9

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.

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.

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. 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.

<u>Recommendations 11, 12, and 14</u>
ACS MIS will institute a management review process of existing procedures for deactivating system access of terminated employees.

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

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

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

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will conduct a detailed analysis to determine Backup requirements; Backup type; Backup site location; Equipment needed; and Staff requirements.	Aryeh Norensberg, Network Services Director	06/01/03	12/31/03		
ACS MIS will a submit short-term purchase request within existing budget for required equipment and also submit a long-term additional funding request for required equipment.		01/01/04	03/31/04		
ACS MIS will develop short-term and long-term testing plans and procedures.		01/01/04	06/30/04		
ACS MIS will setup backup/recovery equipment		07/01/04	09/30/04		
ACS MIS will conduct comprehensive tests of the plan and schedule annual tests as required.		10/01/04	01/31/05		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

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.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
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.	Aryeh Norensberg, Network Services Director Anil Sharma, IT Architecture and Planning Director	Ongoing	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 3: ACS should activate the Callback function contained in the Cisco software.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
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.	Aryeh Norensberg, Network Services Director	Ongoing	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

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.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
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.	Michel Perec, Facilities Design, Construction and Inspection Director	12/24/02	03/10/03		The smoke detector installation was conducted and completed while the Comptroller's Audit was in progress.
The date for FDNY inspection and testing is pending.		Pending	Continuing		
MIS staff training will follow.		Pending	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 5: 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		DOCUMENTATION	COMMENTS
		START	END		
An electrical vendor has submitted a proposal to ACS Facilities for gas/fire suppression for the Data Center.	Michel Perec, Facilities Design, Construction and Inspection Director	04/28/03	Pending		Work commencement will depend upon funding availability.

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 6: ACS should conduct an annual inventory reconciliation of all its computer equipment.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will conduct a baseline inventory of all desktop computer equipment in all of its sites.	David Taylor-Fink, MIS Inventory Director	11/01/02	02/28/03		The baseline inventory was conducted and completed while the Comptroller's Audit was in progress.
ACS MIS will enter baseline inventory data into Track IT! – the ACS MIS inventory management repository.		04/07/03	04/11/03		
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.		04/14/03	Continuing		

**ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES
OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114**

RECOMMENDATION # 7: ACS should affix identification tags to all of its computer equipment.

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 will conduct research and planning, draft and finalize tag language design, and determine cost estimate for purchase request.	David Taylor-Fink, MIS Inventory Director	02/01/03	06/30/03		
ACS MIS will implement an affix of identification tags to all of ACS' computer equipment.		07/01/03	09/30/03		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

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

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
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.	David Taylor-Fink, MIS Inventory Director	06/01/03	12/31/03		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION #9: ACS should conduct an annual inventory reconciliation of all of its software licenses.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
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.	David Taylor-Fink, MIS Inventory Director	06/01/03	12/31/03		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 10: 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		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will activate the feature to ensure that users are prompted to change their passwords every 90 days.	Aryeh Norensberg, Network Services Director	06/01/03	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 11: ACS should establish and implement formal procedures for deactivating system access of terminated employees.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will institute a management review process of existing procedures for deactivating system access of terminated employees.	Ken Clark, Network Services Deputy Director	Ongoing	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT NUMBER: 7F03-114

RECOMMENDATION # 12: ACS should disconnect remote access of users after a specified number of failed login attempts.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will activate the feature to disconnect remote access of users after three (3) login attempts.	Ken Clark, Network Services Deputy Director	Ongoing	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 13: ACS should monitor the activities of users with Domain Administrator access in accordance with Directive 18.

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

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		DOCUMENTATION	COMMENTS
		START	END		
ACS MIS will institute a periodic management review process to monitor the activities of users with Domain Administrator access.	Aryeh Norensberg, Network Services Director Jack Tennyson, Deputy Director Internal Audit	Ongoing	Continuing		

ADMINISTRATION FOR CHILDREN'S SERVICES AUDIT IMPLEMENTATION PLAN
NEW YORK CITY COMPTROLLER'S FOLLOW-UP AUDIT ON DATA PROCESSING CONTROLS AND PROCEDURES OF THE ADMINISTRATION FOR CHILDREN'S SERVICES
AUDIT NUMBER: 7F03-114

RECOMMENDATION # 14: ACS should develop and implement 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		DOCUMENTATION	COMMENTS
		START	END		
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.	Ken Clark, Network Services Deputy Director	Ongoing	Continuing		