AUDIT REPORT

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

Audit Report on the Controls of the Administration for Children's Services Over Personally Identifiable Information

7A09-108

December 10, 2009

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 audited the controls of the Administration for Children's Services (ACS) over personally identifiable information.

ACS protects children from abuse and neglect. It investigates child abuse and neglect reports, provides preventive services and foster care, and helps arrange adoptions. Among the types of data that ACS collects, processes, stores, and transmits is sensitive and confidential personally identifiable information. We audit systems and technological resources of City agencies such as this as a means of ensuring that they are efficient, secure, and operate in the best interest of the public.

The results of our audit, which are presented in this report, have been discussed with officials of ACS, and their comments have been considered in preparing this report. Their complete written response is attached to this report.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please e-mail my audit bureau at audit@Comptroller.nyc.gov or telephone my office at 212-669-3747.

Very truly yours,

William C. Thompson

William C. Thompson, Jr.

WCT/fh

Report: **7A09-108**
Filed: **December 10, 2009**

Table of Contents

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

Audit on the Controls of the Administration for Children's Services Over Personally Identifiable Information
7A09-108

AUDIT REPORT IN BRIEF

The New York City Administration for Children's Services protects children from abuse and neglect. During Fiscal Year 2008, it investigated child abuse and neglect reports involving approximately 90,000 children, provided preventive services to approximately 32,000 children, provided foster care for approximately 17,000 children through 36 foster care agencies City-wide, and helped arrange for the adoption of approximately 1,200 children. ACS also funds and supports 257 Head Start centers and 75 preventive agencies, and enrolls approximately 102,000 children in child care programs.

In carrying-out its mission, ACS collects, processes, stores, and transmits many types of case-record information from its clients and governmental agencies. Data is a critical asset of ACS, and it contains personal information pertaining to every case processed by the agency. One of the types of data at risk of theft or misuse is Personally Identifiable Information (PII). This information contains data that is confidential or sensitive in some way, because it includes individuals' names, addresses, social security numbers, medical information, and other personal information. Disclosure of this information to unauthorized individuals may result in criminal activities, such as identity theft or other inappropriate uses of the information.

Audit Findings and Conclusions

ACS has adequate controls over storage of personally identifiable information it has collected. In addition, its Information and Internet Security Policy defines personnel responsibilities to protect personal information on its systems. Further, ACS has guidelines (the William Bell Policy) requiring that personnel have proper authorization before destroying or removing documents under its stewardship. Moreover, the ACS Division of Personnel (Personnel) places case records in a securely locked area, which includes file cabinets and storage rooms. Finally, we observed that Personnel had shredding bins for the disposal of copies of original documents, as required in ACS guidelines. Also, ACS follows DORIS (Department of Records and Information Services) retention and disposal standards.

However, ACS has an inadequate password policy for its local network and handheld Blackberry devices. The lack of adequate policies and procedures for the local network poses a threat to the security of ACS personal information by unauthorized personnel or other inappropriate parties. We found 15 instances in which the access of terminated employees was not removed or disabled in the ACS computer environment. Also, throughout its information processing systems ACS has not met the requirements of DoITT's (Department of Information Technology and Telecommunications) policies concerning personal information protection. Specifically, ACS does not follow the DoITT Data Classification Policy requiring the classification of data into public, sensitive, private, and confidential categories. In addition, ACS did not ensure that its disaster recovery team members were familiar with its disaster recovery plan and periodically review the necessary steps codified in the plan.

Audit Recommendations

To address these issues, we make 12 recommendations, including that ACS should:

- Immediately send out the data classification survey to all the remaining divisions in order to continue the implementation process of the DoITT Data Classification Policy.
- Complete the data classification process of classifying data collected by each division to ensure the confidentiality, integrity, and availability of ACS personal information.
- Revise its password policy and require passwords to contain at least eight characters.
- Ensure that the access of employees whose services are terminated is removed from the ACS system on a timely basis.
- Create a record-booking process to keep accurate track of dates employee access is removed from the system.
- Require ACS staff who use a Blackberry for work purposes to take the necessary security precautions to protect critical information and to prevent access by unauthorized individuals.

INTRODUCTION

Background

The New York City Administration for Children's Services protects children from abuse and neglect. During Fiscal Year 2008, it investigated child abuse and neglect reports involving approximately 90,000 children annually, provided preventive services to approximately 32,000 children, provided foster care for approximately 17,000 children through 36 foster care agencies City-wide, and helped arrange for the adoption of approximately 1,200 children. ACS also funds and supports 257 Head Start centers and 75 preventive agencies, and enrolls approximately 102,000 children in child care programs.

In carrying-out its mission, ACS collects, processes, stores, and transmits many types of case-record information from its clients and governmental agencies. Data is a critical asset of ACS, and it contains personal information pertaining to every case processed by the agency. One of the types of data at risk of theft or misuse is Personally Identifiable Information (PII). This information contains data that is confidential or sensitive in some way, because it includes individuals' names, addresses, social security numbers, medical information, and other personal information. Disclosure of this information to unauthorized individuals may result in criminal activities such as identity theft or other inappropriate uses of the information.

The unintended disclosure of personal information can result in a number of ways: loss of backup computer tapes, Universal Serial Bus drives, and laptop computers; exposure through Web site attacks; unsecured or inappropriate e-mail exchanges or by other electronic communications or data storage exposures. Disclosure can also occur through the inappropriate disposal of paper files. There have been some high profile reports about personal information being lost as a result of poor stewardship of personal data by organizations.

Several government and private organizations have been tracking data breaches[1] to determine the risks and trends associated with those violations of personal information security. The nonprofit consumer information and advocacy organization Privacy Rights Clearing House (PRCH) started tracking PII incidents and found that for over a four-year period (January 2005–June 2009) more than 200 million total records containing sensitive personal information involving U.S. companies and government agencies were at risk. (See Appendix I.)

Widespread use of computerized recordkeeping and growth in the use of the Internet to collect and share information has resulted in public concern about the privacy of personal information collected by the government. These concerns include those related to the government's ability to ensure the accuracy and confidentiality of information about individuals and prevent misuse of personal information. The City of New York takes responsibility for the protection of PII that it collects while providing municipal services to the public. All employees and contractors with access to City information-processing systems are required to read and

[1] According to the U.S. Government Accountability Office (GAO), the term "data breach" generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information.

acknowledge the Department of Information Technology and Telecommunications' (DoITT) User Responsibilities policy prior to being allowed access to City information systems.

In 1981, Mayoral Directive 81-2 charged the Department of Investigation (DOI) with the responsibility to establish City-wide standards for IT security to ensure that programs, data files, data communications, and City computer systems are used in compliance with this directive. To accomplish this task, in 1998 DOI created the City-wide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE). CISAFE was responsible for the creation, development, and enforcement of consistent and cost-effective security procedures, standards, and controls to ensure the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City of New York. Later, in a Memo of Understanding dated August 8, 2006, between DoITT and DOI, DoITT became responsible for the formulation of security policies and the publication of City-wide information security policies and standards that all agencies and employees, and all contractors and vendors doing business with the City must follow.

By 2008, DoITT addressed how City agencies should protect business information assets. It did so through the release of several policies that requires City agencies and vendors to have: an appropriate level of data and facility protection, an assessment to determine the value of the information being maintained, the appropriate requirements for security to protect City data resources and ensure their integrity and compliance with laws and regulations. Also, the goal of the Municipal Records Management Division of the City's Department of Records and Information Services (DORIS) is to ensure the maintenance of records having continuing administrative and legal value and the retirement or proper disposal of records no longer in current use.

There has never been a comprehensive review of efforts by City agencies to determine whether there are adequate controls in place to safeguard personal information. Given the inherent risks of inadequately protecting personal information, we have initiated a series of audits of City agencies to review and evaluate the sufficiency of their security and other controls over personal information they maintained.

Objectives

The objective of this audit is to determine whether ACS:

- Has adequate controls over personally identifiable information being collected and stored,
- Is properly securing personal information from unauthorized personnel,
- Has followed DoITT's policies to ensure that personally identifiable information is being protected throughout its information processing systems.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

Our fieldwork was conducted from November 2008 to May 2009. To achieve our audit objectives, we interviewed various ACS officials[2] to obtain background on their information protection processes and controls. We received a copy of ACS case record guidelines for the Child Protection division and the list of documents that are included in the case records. Of the 8 divisions interviewed, we noted that these divisions collect information from clients who could be considered sensitive. (See Appendix III.)

The information obtained from these interviews was also used to determine whether City information security policies and procedures were in place and being followed, and to determine the overall security awareness of ACS personnel responsible for safeguarding the agency's personal information. In addition, we:

- Reviewed relevant DoITT policies and City laws regarding the collection of and security controls over personal information by ACS, including statutory requirements when such information is breached.

- Reviewed and analyzed ACS's *Information and Internet Security Policy* to determine whether ACS incorporated DoITT policies concerning the security of data.

- Examined and evaluated the agency's *Data Classification Policy Implementation Plan* and a Data Classification Survey Log provided by ACS to determine whether the agency is complying with DoITT policies, which ensure the agency data is appropriately categorized, used, and protected to perform its mission.

- Reviewed and evaluated the ACS employee training manuals for the Warehouse Inventory Tracking System (WITS) and the Legal Tracking System (LTS) to determine whether ACS has procedures in place to keep track of their case information.

- Reviewed the ACS off-site shredding contract, which contains the procedures for the destruction and disposal of personal information held by ACS.

[2] We interviewed officials from 8 divisions in ACS, which included Childcare and Head Start, Child Protection, Family Court Legal Services, Family Permanency, Quality Assurance, Family Support Services, Financial Services and Administration, which include MIS, Case Records Management and Personnel units.

- Reviewed and analyzed the agency's policies for incidence response in the *Computer Security Incident Response Planning* and *Incident Handing Procedures Draft* to determine whether ACS is complying with DoITT policies regarding security breaches.

- Reviewed and inspected security reports from security software (Websense, NetForensics, ACS's Firewall logs, and McAfee Foundstone Enterprise) that are in place to monitor agency systems to ascertain whether there have been any security breaches.

- Reviewed and inspected ACS's Helpdesk Tickets logs, which provide information on computer related issues that its employees report to its support division for resolution.

- Determined whether the ACS password policy and procedures comply with DoITT's security directives.

- Compared the ACS personnel list of terminated employees with the ACS Management Information System (MIS) list of accounts disabled as of February 2009 to determine whether ACS employee access is removed upon termination of employment.

- Reviewed and analyzed DORIS Guidelines, Policies, and Procedures to determine ACS compliance.

- Reviewed and analyzed the policies in the *Personnel Manual for the Employees of the Administration for Children's Services*[3] to determine whether ACS is complying with DoITT policies.

- Inspected file cabinets and unattended rooms containing case-record information at the Child Care and Head Start, Child Protection, Family Court Legal Services, and Family Permanency Services divisions to test compliance with ACS internal William Bell Policy, a confidential policy related to the retention and disposal of ACS documents, to determine whether ACS is following the necessary procedures.

- Examined ACS disaster recovery and contingency planning procedures for compliance with DoITT directives.

As criteria, we used the DoITT's City-wide Information Security Directives and Policies, the National Institute of Standards and Technology (NIST) *Generally Accepted Principles and Practices for Securing Information Technology System*, the New York City Comptroller's Internal Control and Accountability Directive #18, "Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems," Personal Privacy Protection Law, DORIS Guidelines, Policies, and Procedures, Cyber Security Policy P03-002 (2005),

[3] The *Personnel Manual for the Employees of the Administration for Children's Services* includes the following policies: General Rules and Responsibilities, General Information, Code of Conduct, Staff Ethics, and Standards of Conduct.

Taxpayer Browsing Protection Act, ACS Information and Internet Security Policies, and New York City Charter Chapter 72, §3004.4 (d).

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 was discussed at an exit conference held on October 19, 2009. We submitted a draft report to ACS officials with a request for comments on October 27, 2009. We received a written response from ACS on November 18, 2009. In their response, ACS officials generally agreed with the findings and recommendations of this audit.

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

FINDINGS AND RECOMMENDATIONS

ACS has adequate controls over storage of personally identifiable information it has collected. In addition, its Information and Internet Security Policy defines personnel responsibilities to protect personal information on its systems. Further, ACS has guidelines (the William Bell Policy[4]) requiring that personnel have proper authorization before destroying or removing documents under its stewardship. Moreover, the ACS Division of Personnel (Personnel) places case records in a securely locked area, which includes file cabinets and storage rooms. Finally, we observed that Personnel had shredding bins for the disposal of copies of original documents, as required in ACS guidelines. Furthermore, ACS follows DORIS retention and disposal standards.

However, ACS has an inadequate password policy for its local network and handheld Blackberry devices. The lack of adequate policies and procedures for the local network poses a threat to the security of ACS personal information by unauthorized personnel or other inappropriate parties. We found 15 instances in which the access of terminated employees was not removed or disabled in the ACS computer environment. Also, ACS has not met the requirement of DoITT's policies[5] concerning personal information protection throughout its information processing systems. Specifically, ACS does not follow the DoITT Data Classification Policy requiring the classification of data into public, sensitive, private, and confidential categories. In addition, while ACS had identified disaster recovery team members who were not familiar with the disaster recovery plan or who did not periodically review the steps in the plan, it provided no evidence that it had corrected these weaknesses.

Classification of Data Has Not Been Established

The Data Classification process is critical to protecting the personal information held by ACS. DoITT's Data Classification Policy states that agencies should "ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection." ACS has not complied with DoITT's Data Classification Policy requiring the classification of data into public, sensitive, private, and confidential categories.

DoITT's Data Classification Policy states, "all information at the City of New York and corresponding agencies will be classified at one of four levels: Public, Sensitive, Private, or Confidential." DoITT's policy also requires that the agency have a data steward that is responsible for its data, that data is labeled appropriately based on the four levels of classification, and that data classified as private and confidential be protected. While ACS has established a procedure for implementing DoITT's Data Classification Policy, it has not completed the process of classifying and protecting its data pursuant to DoITT's policy.

[4] The William Bell Policy states that ACS must follow the guidelines included in the Model Case Record, which is a comprehensive list of documents that may be included in case records.

[5] See Appendix II.

In December 2008, after our audit began, ACS commenced implementing the Data Classification Policy by distributing DoITT's IT data classification survey to 8 out of 11 major operating divisions.[6] By March 13, 2009, ACS had received the results from these initial surveys and is currently reviewing the information obtained from the surveys. However, ACS officials have yet to send the survey to the remaining divisions. The survey provided just an inventory of the data collected by each division. ACS indicated that they are only up to step 3 of an 11-step ACS Data Classification Policy Implementation Plan. ACS plans to complete the Data Classification survey by December 2009.

By not adhering to DoITT's policy and classifying data accordingly, ACS is unable to determine how to adequately protect the data and personal information under its supervision. As a consequence, ACS does not have adequate controls over its personal information and may be susceptible to loss of personal information or theft.

Recommendations

ACS should:

1. Immediately send the data classification survey to all the remaining divisions in order to continue the implementation process of the DoITT Data Classification Policy.

ACS Response: "Partial compliance. Nine Divisions completed the classification survey by March 2009. The remaining Divisions will complete the survey by the end of December 2009."

2. Complete the data classification process of classifying data collected by each division to ensure the confidentiality, integrity, and availability of ACS personal information.

ACS Response: "Partial compliance. ACS will continue with the implementation of the Data Classification Plan that has been developed internally. The ACS Commissioner and the DoITT Commissioner have discussed the DoITT policy and have agreed to have ACS work jointly with DoITT on this issue. ACS will reach out to DoITT to develop a strategy on implementation and to determine how best to move forward."

Auditor Comment: ACS plans to complete the survey by the end of December 2009 but has not provided a timeline that indicates a date to complete the implementation process of the DoITT Data Classification Policy.

[6] The 8 divisions are: ACS Childcare and Head Start, Child Protection, Family Court Legal Services, Family Permanency, Quality Assurance, Family Support Services, Policy and Planning, and Financial Services. General Counsel, Community and Government Affairs, and Administration did not receive the survey. However, three sub-units of Administration division completed the survey.

Security over Personal Information

ACS has an Information and Internet Security Policy that defines users' responsibilities for protecting personally identifiable information on all ACS information processing systems. There is also an incident response policy that provides procedures for monitoring information security incidents, such as data breaches. ACS has a password policy in place for the Child Care Review System and the CONNECTIONS system on the state network.

However, ACS is not complying with the DoITT Password Policy and has an inadequate password policy for its local network and handheld Blackberry devices. It does not require users to change their passwords after 90 days, and it does not disable a user's access to the network after a predetermined number of unsuccessful log-in attempts. We also found 15 instances in which the access of terminated employees was not removed or disabled in the ACS computer environment.

Lack of Password-Security Controls

ACS is not following DoITT's Password Policy to ensure the security of personal information. The DoITT's Password Policy states, "Passwords and/or PINs must have a minimum length of eight (8) characters." However, ACS Information and Internet Security Policy states, "For ACS passwords the Security Supervisor will create an account that is not less than 6 characters and no more than 14." Since ACS password policy allows for the use of 6 or 7 characters for its passwords, ACS is not complying with DoITT's policy, thus posing a threat to the personal information it has collected and stored on its systems.

We also found that ACS personnel change their passwords after 90 days for the New York State information systems. ACS does not have an adequate policy and procedure to ensure the security of the ACS local network and is therefore not in compliance with DoITT's Password policies, which state:

- "Screen lock must be activated within fifteen (15) minutes of unattended inactivity." Not enabled on the ACS local network.

- "Passwords and/or PINs must be changed at least every ninety (90) days." Not systematically done on the ACS local network and peripheral computing devices, i.e., Blackberries and laptops.

- "All accounts that provide access to sensitive, private or confidential Information must be automatically disabled after five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes."

The lack of adequate policies and procedures for the local network poses a threat to the security of ACS personal information from unauthorized personnel or other inappropriate parties.

Access for Terminated Employees Not Disabled

Comptroller's Directive #18, 8.1.2, states, "Active password management includes: Deactivation of inactive user accounts and accounts for employees whose services are terminated." We found that access to the ACS computer environment had not been disabled for some terminated employees of the agency. Specifically, we found that 15 of 64 terminated employees did not have their access to the system disabled. ACS provided us with a list of 64 employees whose service was terminated in February 2009. Personnel indicated that it sends a daily notification to the MIS to remove terminated employees from access to the system. ACS also provided us with a list from MIS indicating employees disabled from the ACS system. We noted that MIS has no record or tracking system of when it received these notifications from Personnel. Also, MIS does not keep track of the dates that employees' access was removed from the ACS system.

DoITT Directive 2.3, §3.5, states, "In the case of employee termination. . .this notification may be by telephone, by e-mail, or in person, but must be followed up with formal written notification to the system administrator within three (3) business days." By not removing the access of terminated employees from the system, ACS creates significant risk of unauthorized access to the system and exposure and misuse of confidential personal information.

Recommendations

ACS should comply with DoITT policy and:

3. Revise its password policy and require passwords to contain at least eight characters.

ACS Response: "Full compliance as of June 2009. Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the eight character password, since June 2009."

4. Create a lockout feature to the system that is activated within 15 minutes of unattended inactivity by employees.

ACS Response: "Full compliance as of June 2009. Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with all DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with the DoITT security policies, including the lockout feature, since June 2009."

5. Require employees to change their passwords at least every 90 days.

ACS Response: "Full compliance as of June 2009. Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been incompliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the 90 day change of password policy, since June 2009."

6. Ensure that all accounts be automatically disabled after five sequential, invalid login attempts within a 15-minute period.

ACS Response: "Full compliance as of June 2009. Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the feature that automatically disables use after five sequential, invalid log-in attempts within a 15-minute period, since June 2009."

7. Ensure that the access of employees whose services are terminated is removed from the ACS system on a timely basis.

ACS Response: "Full compliance as of March 2009. In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that accesses of employees whose services have been terminated are removed from the ACS system on a timely basis."

Auditor Comment: We found 15 of 64 terminated employees whose access to the system was not disabled as of February 2009. During our fieldwork and the exit conference, ACS did not provide any documentation indicating that it has taken these 15 terminated employees off the system.

8. Create a record-keeping process to keep accurate track of dates employee access is removed from the system.

ACS Response: "Full compliance as of March 2009. In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that accesses of employees

whose services have been terminated are removed from the ACS system on a timely basis. The system tracks the dates that employees are removed from ACS systems."

Auditor Comment: During our fieldwork and at the exit conference, ACS did not provide any documentation indicating that it has implemented an automated employee-separation tracking system.

Lack of Controls over Information on Blackberry Handheld Devices

ACS has 884 Blackberry handheld devices, which may contain confidential information and that are distributed to certain employees to access their e-mail. ACS does not have a policy in place that requires employees to use a password or PIN to protect the information on the Blackberry devices. DoITT User Responsibility Policy specifies that, "PINs for Blackberry, PDA, and voicemail must be a minimum of four (4) digits."

DoITT's Portable Data Security Policy states: "All portable computing devices used to process and store City of New York information must be physically protected and appropriate security measures provided for the data contained." This policy also states that laptop computers, personal computers, smart telephones, Blackberry devices, and PDAs should not store or transmit information classified as "Confidential" unless devices are in compliance with City of New York Information Security Policies. ACS indicated that it is only now in the process of creating such a policy. Therefore, in the event that any of the Blackberry devices is lost or stolen or the unprotected information is compromised through unauthorized access, ACS is at risk of losing confidential personal information.

Recommendations

ACS should comply with DoITT policy and:

9. Require ACS staff who use a Blackberry for work purposes to take the necessary security precautions to protect critical information and to prevent access by unauthorized individuals.

ACS Response: "ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009."

10. Install a password or PIN function for the protection of personal information that is accessible by Blackberry devices.

ACS Response: "ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009."

Disaster Recovery Plan Should Be Reviewed

ACS provided us with a draft of its Disaster Recovery Mitigation Plan. ACS indicated that its draft disaster recovery plan is a "living document"[7] that is periodically updated. ACS provided us with its signed-off last draft sent to DoITT for review on November 26, 2008. The plan requires that ACS's disaster recovery team be properly trained and prepared so the agency can continue to perform critical functions in case of a disaster or an emergency. The last disaster recovery test was performed on December 12, 2008. The MIS team reviewing the test and the plan recommended that team members need to be more familiar with the disaster recovery plan and should practice their roles outlined in the plan. Moreover, as the disaster recovery plan is a "living document," team members should periodically review the plan to be familiar with any revised steps and changes made to the plan. ACS informed us that it had addressed these weaknesses but did not provide evidence for that claim.

Recommendation

ACS should:

11. Require its recovery team members to periodically review the necessary steps in the disaster recovery plan so they are properly prepared in case of a disaster.

ACS Response: "Full compliance since 2006. ACS implemented an IT Services Disaster Recovery Plan in 2006 that requires periodic review, update and training for team members to ensure that they are properly prepared in the case of a disaster. As part of the Recovery Plan, team members participate in a Disaster Recovery Plan testing twice a year. During the testing period, ACS conducts a review and self assessment to determine and correct any weaknesses in implementing the Recovery Plan. The Plan is reviewed with team members and team members are trained during the test period twice a year."

Auditor Comment: ACS indicates that it implemented an IT Services Disaster Recovery Plan in 2006 that requires training for team members to ensure they are properly prepared in the case of a disaster. However, we found that the recovery test performed on December 2008 again demonstrated that its recovery team members needed periodic reviews of the necessary steps in the disaster recovery plan.

[7] A "living document" implies that the plan will constantly evolve and not remain stagnant due to the everyday changes that occur in business.

Other Issues

ACS Has Not Performed an Annual Policy Review

ACS Information and Internet Security Policy states that a complete policy review and audit will be performed no less that once a year. These audits take place in an unannounced fashion, focusing on specific policy. The policy states, "The use of internal and 3rd party audits to ensure policy and procedure compliance is highly recommended . . . third party review is essential for an unbiased assessment of the agency infrastructure, policy and procedure." However, ACS has not performed an annual policy review.

Recommendation

ACS should:

12. Immediately perform a complete policy review to ensure that it is comprehensive in nature and complies with DoITT's policies and procedures.

ACS Response: "ACS MIS is conducting a comprehensive GAP Analysis [a tool that helps a company to compare its actual performance with its potential information] of all DoITT security policies published prior to July 29, 2008. As a result of the GAP Analysis ACS has completed the following: Anti Virus - Full Compliance, Password Policy Local Networks - Full Compliance, Blackberry - Full Compliance by Dec 2009, Database Management - Partial compliance implementation in progress, Data Classification Implementation in progress."

Auditor Comment: ACS has not performed an annual policy review by a third party. The ACS Information and Internet Security Policy states, "The use of internal and third party audits to ensure policy and procedure compliance is highly recommended . . . [and] third party review is essential for an unbiased assessment of the agency infrastructure, policy and procedure." ACS should have a third party perform a complete policy review in addition to the review of MIS.

Appendix I

Privacy Clearing House Security Breaches

Date Made Public	Location	Type of Data Breach	# Records Affected
June 7, 2009	T-Mobile USA (Bellevue, WA)	T-Mobile USA is looking into claims that a hacker has broken into its data bases and stolen customer and company information. Someone anonymously posted the claims on the security mailing list Full Disclosure. In that post, the hacker claims to have gotten access to "everything, their databases, confidential documents, scripts and programs from their servers, financial documents up to 2009." The hacker has been in touch with the carrier's competitors, trying to sell the data, but has been unsuccessful, so now is looking to hawk the data to the highest bidder.	Unknown*
May 21, 2009	Internal Revenue Service (several IRS document disposal facilities in the U.S.)	The U.S Treasury Inspector General for Tax Administration found in a Fiscal Year 2008 audit that in more than a dozen IRS document disposal facilities, old taxpayer documents were being tossed out in regular waste containers and dumpsters. In addition, the investigation found that IRS officials failed to consistently verify whether contract employees who have access to taxpayer documents had passed background checks. Further, investigators had difficulty finding anyone responsible for oversight of most of the facilities that the IRS contracted with to burn or shred sensitive taxpayer documents. The review was performed at IRS offices in Phoenix, Tempe, and Tucson, Arizona; New Carrollton, Maryland; Holtsville, Garden City, and Westbury, New York; and Ogden, Utah, and included questionnaires to 14 Territory Managers across the country during the period September 2007 through May 2008.	Unknown
May 19, 2009	National Archives (College Park, Md)	The National Archives lost a computer hard drive containing massive amounts of sensitive data from the Clinton administration, including Social Security numbers, addresses, and Secret Service and White House operating procedures. The Archives had been converting the Clinton administration information to a digital records system when the hard drive went missing. The hard drive was left on a shelf and unused for an uncertain period of time. When the employee tried to resume work, the hard drive was missing.	Unknown
May 5, 2009	Fulton County Board of Registration and Elections (Atlanta, GA)	Boxes were found in a trash bin at Atlanta Technical College. They contained about 75,000 voter registration application cards and 24,000 precinct cards. Many of the documents contained personal information on active voters, such as full names and Social Security numbers.	99,000

*At the present time, the approximate number of records that have been compromised due to security breaches could not be determined.

Appendix II

List of DoITT Policies and Directives Used and ACS Compliance

DoITT Policies and Directives	ACS Compliance	Reasons/Comments
Data Classification Policy	No	Does not classify data into public, sensitive, private, and confidential categories. Completed only step 3 of 11 step procedures.
Identity Management Policy	No	1. Password controls weakness. 2. Terminated employees still have access to ACS systems.
Incident Response Policy	Yes	
Password Policy	No	1. Password does not have a minimum length requirement of 8 characters. 2. Does not require users to change their passwords every 90 days. 3. Does not disable a user's access to network after a predetermined number of unsuccessful log-in attempts. 4. No lockout feature that is activated within 15 minutes of unattended inactivity by employees.
Personnel Security Policy	Yes	
Portable Data Security Policy	No	No security password for Blackberry
Security Accreditation Process	No	Does not classify its data
User Responsibility Policy	No	No Password/PIN for Blackberry
City-wide Information Security Policy	Yes	
Database Management Systems Directive	No	Does not require users to change their password as defined in the policy and the passwords do not have a minimum length requirement of 8 characters.
Directory Services Directive	Yes	
Disposal of Information Assets Directive	Yes	
Incident Response Directive	Yes	
Risk Assessment Directive	Yes	
User Account Management Directive	No	Does not send notification to MIS to remove terminated employees from the system on a timely basis.

Collected Information from ACS Divisions That Could Be Considered Sensitive

Quality Assurance's function involves the quality assurance of Child Protection. It performs sample reviews of cases. The Quality Assurance staff can obtain a hard copy of records and base their samples on the hard copies. Staff are responsible for a standard evaluation of case records. They do not take personal information off-site. They have read-only access to the New York State system CONNECTIONS and are not allowed to enter information into CONNECTIONS.

Family Permanency is responsible for providing assistance to contracted agencies that provide services to children. Family Permanency has access to three IT systems: Child Care Review System and CONNECTIONS on the state network, and Legal Tracking System on the local network. They also use the WITS for the storage of their case records. The case records are catalogued, coded, and the information is entered into WITS.

Child Protection protects children that are abused or receive maltreatment. Only after a case has begun will staff collect information on the parent and the child. Child Protection uses the CONNECTIONS system and enters information that they collect. ACS said it receives Social Security numbers, which become part of its case record information. These records are kept on-site for two years in locked file cabinets or locked office rooms.

Child Care determines eligibility, gathers information from parents, enrolls children in programs, and provides program oversight. They use only the Automated Child Service system. The critical information collected is income, relationship between the child and parent, names (child, parents and other associated family members), and children's social security number. Head Start utilizes the Employee Tracking System, which is a Web-based application. Head Start provides about 76 programs, which include grant programs and educational services. Files are placed in secure cabinets only and the cabinets are kept under lock and key. Human Resources staff have access to these files.

Family Court Legal Services is responsible for representing ACS in child neglect and abuse cases, permanency hearings, and other child welfare proceedings in the New York City Family Courts. They use the LTS and file cases in the Family Court, which includes foster care and supervision. ACS receives personal information such as client information, which includes a child's name and records.

Family Support Services provides preventive services, parenting education, and homemaking services to families throughout New York City and provides a range of support services to contract agencies. ACS said all of their records have critical information, which includes addresses, social security numbers, and other personal information. Information that is collected is entered into the CONNECTIONS system, and employees receive different levels of access, depending on their job function.

Financial Services is made up of Budget, Payment, Claims, and Audit departments. These four departments are responsible for conducting the financial activities of the agency and ensuring that all financial processes are carried out in full accordance with City, state and federal guidelines. The Payment department has different levels of access to the Financial Management System (FMS). They keep files that are needed for claims for two years, which is the maximum amount of time to file a claim. Payment has an adoption subsidiary that contains children's information and is kept in locked file cabinets for two years on site.

The Administrative division includes Case Records Management, Personnel Department, and other units. Case Records Management uses the WITS for the storage of cases that are deemed closed. These cases are picked up by the contractor and sent to the off-site warehouse for storage. Case Records staff said they have been using the same vendor, and the boxes have been stored at their warehouse for several years. The Personnel Department is responsible for hiring, recruitment, title change, promotions of employees, payroll, and timekeeping. The systems used are Payroll Management System (PMS), CityTime, and the New York City Automated Personnel System (NYCAPS). Personnel staff said that ACS employees use Blackberries for viewing their e-mails. These e-mails include attachments that may contain confidential information.

Administration for Children's Services

Susan Nuccio
Deputy Commissioner/
Chief Financial Officer
Financial Services

150 William Street
10th Floor
New York, NY 10038

Email Address:
susan.nuccio@dfa.state.ny.us

November 10, 2009

Mr. John Graham
Deputy Comptroller
Audits, Accountancy & Contracts
City of New York Office of the Comptroller
Executive Offices
1 Center Street
New York, New York 10007-2341

Re: Audit Report on the Controls over Personally Identifiable Information by the Administration for Children's Services 7A09-108

Dear Mr. Graham:

Attached please find ACS' response to the Draft Report for the above captioned audit. As requested, our response addresses each recommendation made in the audit and includes the corresponding Agency Implementation Plan (AIP).

Sincerely,

Julie Bittman
Director, ACS External Audit

Attachments

RECOMMENDATION # 1 – *ACS should immediately send the data classification survey to all the remaining divisions in order to continue the implementation process of the DoITT Data Classification Policy.*

ACS RESPONSE
Partial compliance.

Nine Divisions completed the classification survey by March 2009. The remaining Divisions will complete the survey by the end of December 2009.

RECOMMENDATION # 2 – *ACS should complete the data classification process of classifying data collected by each division to ensure the confidentiality, integrity and availability of ACS personal information.*

ACS RESPONSE
Partial compliance.

ACS will continue with the implementation of the Data Classification Plan that has been developed internally. The ACS Commissioner and the DoITT Commissioner have discussed the DoITT policy and have agreed to have ACS work jointly with DoITT on this issue. ACS will reach out to DoITT to develop a strategy on implementation and to determine how best to move forward.

RECOMMENDATION # 3 – *ACS should comply with DoITT policy and revise its password policy and require passwords to contain at least eight characters.*

ACS RESPONSE
Full compliance as of June 2009.

Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the eight character password, since June 2009.

RECOMMENDATION # 4 – *ACS should comply with DoITT policy and create a lockout feature to the system that is activated within 15 minutes of unattended inactivity by employees.*

ACS RESPONSE

Full compliance as of June 2009.

Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with all DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with the DoITT security policies, including the lockout feature, since June 2009.

RECOMMENDATION # 5 – *ACS should comply with DoITT policy and require employees to change their passwords at least every 90 days.*

ACS RESPONSE

Full compliance as of June 2009.

Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the 90 day change of password policy, since June 2009.

RECOMMENDATION # 6 – *ACS should comply with DoITT policy and ensure that all accounts be automatically disabled after five sequential, invalid log-in attempts within a 15-minute period.*

ACS RESPONSE

Full compliance as of June 2009.

Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the feature that automatically disables use after five sequential, invalid log-in attempts within a 15-minute period, since June 2009.

RECOMMENDATION # 7 – *ACS should comply with DoITT policy and ensure that the access of employees whose services are terminated is removed from the ACS system on a timely basis.*

ACS RESPONSE

Full compliance as of March 2009.

In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that accesses of employees whose services have been terminated are removed from the ACS system on a timely basis.

RECOMMENDATION # 8 – *ACS should comply with DoITT policy and create a record-keeping process to keep track of dates employee access is removed from the system.*

ACS RESPONSE

Full compliance as of March 2009.

In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that accesses of employees whose services have been terminated are removed from the ACS system on a timely basis. The system tracks the dates that employees are removed from ACS systems.

RECOMMENDATION # 9 – *ACS should comply with DoITT policy and require ACS staff who use a Blackberry for work purposes to take the necessary security precautions to protect critical information and to prevent access by unauthorized individuals.*

ACS RESPONSE

ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009.

RECOMMENDATION # 10 – *ACS should comply with DoITT policy and install a password or PIN function for the protection of personal information that is accessible by Blackberry devices.*

ACS RESPONSE

ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009.

RECOMMENDATION # 11 – *ACS should require its recovery team members to periodically review the necessary steps in the disaster recovery plan so that they are properly prepared in case of a disaster.*

ACS RESPONSE

Full compliance since 2006.

ACS implemented an IT Services Disaster Recovery Plan in 2006 that requires periodic review, update and training for team members to ensure that they are properly prepared in the case of a disaster. As part of the Recovery Plan, team members participate in a Disaster Recover Plan testing twice a year. During the testing period, ACS conducts a review and self assessment to determine and correct any weaknesses in implementing the Recovery Plan. The Plan is reviewed with team members and team members are trained during the test period twice a year.

RECOMMENDATION # 12 – *ACS should immediately perform a complete policy review to ensure that it is comprehensive in nature and complies with DoITT's policies and procedures.*

ACS RESPONSE

ACS MIS is conducting a comprehensive GAP Analysis of all DoITT security policies published prior to July 29, 2008. As a result of the GAP Analysis ACS has completed the following:

Anti Virus	Full Compliance
Password Policy	Local Networks – Full Compliance Blackberry – Full Compliance by Dec 2009 Database Management – Partial compliance, implementation in progress
Data Classification	Implementation in progress

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 1 – ACS should immediately send the data classification survey to all the remaining divisions in order to continue the implementation process of the DoITT Data Classification Policy.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Nine divisions completed the classification survey by March 2009. The remaining divisions will complete the survey by the end of December 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Nov 2008	Dec 2009	

ADDENDUM
Page 6 of 15

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 2 – ACS should complete the data classification process of classifying data collected by each division to ensure the confidentiality, integrity and availability of ACS personal information.

RESPONSIBLE MANAGER'S NAME - JULIE FRIESEN, Deputy Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
ACS will continue with the implementation of the Data Classification Plan that has been developed internally. The ACS Commissioner and the DoITT Commissioner have discussed the DoITT policy and have agreed to have the ACS work jointly with DoITT on this issue. ACS has reached out to DoITT to develop a strategy on implementation and to determine how best to move forward.	JULIE FRIESEN Deputy Commissioner, Division of Administration	Nov 2008	June 2011	

ADDENDUM
Page 7 of 15

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 3 – ACS should comply with DoITT policy and revise its password policy and require passwords to contain at least eight characters.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Full compliance as of June 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	June 2009	Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies including at least eight characters password since June 2009.

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 4 - ACS should comply with DoITT policy and create a lockout feature to the system that is activated within 15 minutes of unattended inactivity by employees.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Full compliance as of June 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	June 2009	Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with all DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with the DoITT security policies, including the lockout feature, since June 2009.

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 5 – ACS should comply with DoITT policy and require employees to change their passwords at least every 90 days.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Full compliance as of June 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	June 2009	Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the 90 day change of password policy, since June 2009.

RECOMMENDATION # 6 – ACS should comply with DoITT policy and ensure that all accounts be automatically disabled after five sequential, invalid log-in attempts within a 15-minute period.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Full compliance as of June 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	June 2009	Approximately sixty percent of ACS users are served by the New York State local network. That system is operated under NY State IT security policies which comply with all DoITT policy requirements. The ACS State network users have been in compliance with the DoITT password policy requirements since the introduction of this network at ACS. All ACS network users have been fully compliant with all DoITT password policies, including the feature that automatically disables use after five sequential, invalid log-in attempts within a 15-minute period, since June 2009.

RECOMMENDATION # 7 - ACS should comply with DoITT policy and ensure that the access of employees whose services are terminated is removed from the ACS system on a timely basis.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Full compliance as of March 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	Mar 2009	In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that access for employees whose services have been terminated are removed from the ACS system on a timely basis.

RECOMMENDATION # 8 – ACS should comply with DoITT policy and create a record-keeping process to keep track of dates employee access is removed from the system.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		COMMENTS
		START	END	
Full compliance as of March 2009.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Mar 2009	Mar 2009	In March 2009, ACS conducted a review of this process and strengthened its existing manual system to ensure that MIS promptly removes from its IT systems those employees whose services have been terminated by the agency. In October 2009, ACS implemented an automated employee-separation tracking system. The tracking system ensures that access for employees whose services have been terminated are removed from the ACS system on a timely basis. The system tracks the dates that employees are removed from ACS systems.

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 9 – ACS should comply with DoITT policy and require ACS staff who use a Blackberry for work purposes to take the necessary security precautions to protect critical information and to prevent access by unauthorized individuals.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES		COMMENTS
		START	END	
Implementation in progress.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Oct 2009	Dec 2009	ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009.

Administration for Children's Services
AUDIT IMPLEMENTATION PLAN – November 10, 2009
New York City Comptroller's Audit on Controls over Personally Identifiable Information by ACS
Audit Number 7A09-108

RECOMMENDATION # 10 – ACS should comply with DoITT policy and install a password or PIN function for the protection of personal information that is accessible by Blackberry devices.

RESPONSIBLE MANAGER'S NAME - ANIL SHARMA, Acting Assistant Commissioner, Division of Administration

CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PERSON	DATES START	DATES END	COMMENTS
Implementation in progress.	ANIL SHARMA Acting Assistant Commissioner, Division of Administration	Oct 2009	Dec 2009	ACS is working in conjunction with New York State to bring agency users into compliance with DoITT security policies regarding Blackberries. ACS anticipates full compliance with DoITT security guidelines for all agency Blackberry users by the end of December 2009.