City of New York

OFFICE OF THE COMPTROLLER

Scott M. Stringer
COMPTROLLER

AUDITS & SPECIAL REPORTS

IT AUDIT

Marjorie Landa
Deputy Comptroller for Audit

Audit Report on the New York City Administration for Children's Services' Security Controls over Its Personally Identifiable Information at the Division of Preventive Services

SI18-060A
June 22, 2018
http://comptroller.nyc.gov

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
SCOTT M. STRINGER

June 22, 2018

To the Residents of the City of New York:

My office has audited the New York City Administration for Children's Services' (ACS) Division of Preventive Services (DPS) to determine whether it has adequate security controls over personally identifiable information (PII) that is being collected and stored and is properly securing personal information from unauthorized access. We perform audits of this type of the information technology (IT) systems maintained by City agencies such as ACS to help ensure the integrity of the data stored in those systems and to minimize the risk of improper access to the City's systems.

The audit found that ACS has established policies, procedures and guidelines for access control, data protection and data classification to protect PII that is collected and stored by DPS. However, our audit found weaknesses in ACS' access and security controls, including inactive network user accounts that were not disabled, passwords for remote user accounts that never expired and a lack of proper monitoring of external service providers' access to its critical applications. In addition, we found that the agency maintained an inadequate encryption policy for stored data, used outdated operating systems that the manufacturer no longer supports and lacked a formal agency-wide disaster recovery plan for critical applications hosted at ACS' data center. Finally, our field visits to sites operated by external service providers found insufficient physical security over the PII that the providers collected, stored and disposed of.

Based on the audit findings, we made 17 recommendations including that ACS should: ensure that all inactive network user accounts are immediately disabled and periodically review user account activity; develop and implement strong remote-user access policies and procedures; ensure that only authorized users have access to ACS' network; develop formal agency-wide disaster recovery plan for critical applications that are hosted in the ACS data center; and properly store client records in locked secure locations with access limited to only authorized personnel.

The results of the audit have been discussed with ACS officials, and their comments have been considered in preparing this report. ACS' complete written response is attached to this report.

If you have any questions concerning this report, please e-mail my Audit Bureau at audit@comptroller.nyc.gov.

Sincerely,

Scott M. Stringer

DAVID N. DINKINS MUNICIPAL BUILDING • 1 CENTRE STREET, 5TH Floor • NEW YORK, NY 10007
PHONE: (212) 669-3500 • @NYCCOMPTROLLER
WWW.COMPTROLLER.NYC.GOV

TABLE OF CONTENTS

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
AUDITS & SPECIAL REPORTS
IT AUDIT

Audit Report on the New York City Administration for Children's Services' Security Controls over Its Personally Identifiable Information at the Division of Preventive Services

SI18-060A

EXECUTIVE SUMMARY

This audit was conducted to determine whether the New York City Administration for Children's Services' (ACS) Division of Preventive Services (DPS) properly secures personal information from unauthorized access and has adequate security controls over personally identifiable information (PII) that is being collected and stored.

ACS is responsible for protecting the safety and promoting the well-being of New York City's children and strengthening their families by providing child welfare, child care and early education services. DPS is the unit of ACS that oversees the delivery and monitoring of preventive services for children and families in their communities through contracted service providers. Among its services are in-home family counseling, support groups for parents and youth and homemaking services.

To accomplish its varying tasks, DPS uses several specialized computer applications. The agency's critical applications may contain PII that is private, sensitive and/or confidential, including names, addresses, social security numbers and medical information. ACS is responsible for ensuring that security controls are in place to protect PII that is collected and stored.

Audit Findings and Conclusions

The audit found that ACS has established policies, procedures and guidelines for access control, data protection and data classification to protect the PII that is collected and stored by DPS. However, we found several weaknesses in the agency's access controls, including inactive network user accounts that were not disabled and passwords for certain remote user accounts that never expired. In addition, ACS did not comply with the New York City Department of Information Technology and Telecommunications' (DoITT's) *Password Policy* with respect to two critical applications, did not properly monitor external service providers' access to its critical

applications and did not properly limit users' access privileges in its Preventive Organization Management Information System (PROMIS) application.

Further, we found security control weaknesses in ACS' computer environment, including an inadequate encryption policy for stored data and the agency's use of outdated operating systems that the manufacturer no longer supports. ACS provided no evidence that it had addressed reported software vulnerabilities and suspicious activities that required immediate action to prevent potential security breaches, and the agency did not have a formal agency-wide disaster recovery plan for critical applications hosted at ACS' data center. Finally, our field visits to sites operated by external service providers found insufficient physical security over the PII that the providers collected, stored and disposed of.

Audit Recommendations

To address the issues raised by this audit, we make 17 recommendations to ACS, including the following:

- Ensure that all inactive network user accounts are immediately disabled and periodically review user account activity to ensure that only active users and providers have access.
- Develop and implement strong remote-user access policies and procedures, including but not limited to a password-expiration policy that complies with DoITT's standards, to ensure that only authorized users have access to ACS' network.
- Immediately review and reassess all Family Assessment Form System (FAF) and PROMIS user accounts to ensure that each user is currently authorized and needs access.
- Develop a password policy and procedure that requires PROMIS default passwords be changed periodically and comply with DoITT's *Password Policy*.
- Ensure that all private, sensitive and confidential information stored in the database and backup tapes is encrypted.
- Assess all hardware and software in use by the agency and ensure that the versions are up to date.
- Review all users' access to agency information systems and ensure that users are given access to only those features necessary to perform their job duties.
- Develop a formal agency-wide disaster recovery plan for critical applications that are hosted in the ACS data center.
- Properly store client records in locked secure locations with access limited to only authorized personnel.

Agency Response

In its response, ACS agreed with the audit's 17 recommendations. The full text of ACS' response is included as an addendum to this report.

AUDIT REPORT

Background

ACS is responsible for protecting the safety and promoting the well-being of New York City's children and strengthening their families by providing child welfare, juvenile justice, child care and early education services. In carrying out its mission, ACS collects, processes, stores and transmits many types of case-record information.

DPS is the unit of ACS that oversees the delivery and monitoring of preventive services for children and families in their communities through contracted service providers. Preventive services are designed to help families keep their children safely at home. Among its services are in home family counseling, support groups for parents and youth and homemaking services.

To accomplish its varying tasks, DPS uses several specialized computer applications, including PROMIS, FAF, the Family Team Conferencing (FTC) Database System, and the Child Trafficking Database (CTDB). These critical applications may contain PII that is private, sensitive and/or confidential, such as names, addresses, social security numbers and medical information. Lack of proper security over PII may lead to identity theft or misuse of personal data; accordingly, physical security and access controls of such records are essential.

DoITT's Citywide Information Security Policy requires that information stored in an agency's applications be placed in a secured environment and protected from unauthorized access. To accomplish that level of security, adequate access controls, such as user-authorization, identification, authentication, access-approval and login credentials are essential. ACS is responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment.

As the City agency charged with overseeing information technology (IT) and telecommunications for more than 120 City agencies, DoITT provides assistance to help agencies deliver efficient, effective and secure IT services. It provides security expertise and services, and seeks to protect City data and IT assets through proper management of security infrastructure, policies and standards. All City agencies and employees, as well as contractors and vendors doing business with the City, are required to follow these policies and standards.

Objectives

To determine whether the ACS DPS:

- Is properly securing personal information from unauthorized access; and
- Has adequate security controls over personally identifiable information that is being collected and stored.

Scope and Methodology Statement

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 and 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.

The scope of this audit was from September 2017 to April 2018. We conducted fieldwork from October 2017 to April 2018. Please refer to the Detailed Scope and Methodology at the end of this report for the specific procedures and tests that were conducted.

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 and was discussed at an exit conference held on May 30, 2018. The discussions with ACS and its submission of additional information were considered in preparation of the draft report. On June 1, 2018, we submitted a draft report to ACS with a request for written comments. We received a written response from ACS on June 15, 2018.

In its response, ACS agreed with all 17 audit recommendations. The agency stated that, "ACS works with the New York City Department of Information Technology and Telecommunications (DoITT) and the New York State Office of Children and Family Services (OCFS) in development of new systems and building in compliance with New York City DoITT and New York State OCFS policy at the time of construction."

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

FINDINGS AND RECOMMENDATIONS

The audit found that ACS has established policies, procedures and guidelines for access control, data protection and data classification to protect the PII that is collected and stored by DPS. However, we found several weaknesses in the agency's access controls, including the following:

- Inactive network user accounts were not disabled.
- Passwords for some remote user accounts never expired.
- ACS did not comply with DoITT's *Password Policy* for two critical applications, in that it failed to: (1) disable user accounts after five sequential invalid login attempts; (2) implement a timeout feature after 15 minutes of a user's inactivity; and (3) enforce password complexity rules to protect against unauthorized access.
- ACS did not properly monitor access to its critical applications by external service providers.
- Inappropriate access privileges were given to PROMIS users.

Further, we found the following security control weaknesses in ACS' computer environment:

- ACS did not have an adequate encryption policy to protect its data.
- The agency maintained outdated operating systems that the manufacturer no longer supports.
- ACS provided no evidence that it had addressed reported software vulnerabilities and suspicious activities that required immediate action to prevent potential security breaches.

ACS also did not have a formal agency-wide disaster recovery plan for critical applications hosted at ACS' data center. Finally, our field visits to sites operated by external service providers found insufficient physical security over the PII that the providers collected, stored and disposed of. These matters are discussed in detail below.

Network Access Control Weaknesses

ACS has established policies and procedures for protecting its network. However, we found several weaknesses in the agency's access controls, specifically, in its failures to de-provision inactive user accounts and to require its contracted service providers to follow City password-expiration rules when accessing its network.

DoITT's Identity Management Security Policy states that "[u]ser accounts will be created and de-provisioned in a timely manner." In addition, DoITT's *Password Policy* mandates that "User Account passwords and/or PINs must expire at least every 90 days." We analyzed the 11,886 network user accounts ACS listed as current in January 2018 and found that 1,847 of those user accounts had been inactive for periods ranging from over 90 days to 8 years, of which 1,801 were in the names of non-employees, specifically service providers, consultants and interns, who according to ACS' list, still had access to the ACS network. Our tests also found that an additional 974 users with active accounts had never logged into the network since their accounts were created anywhere from over 90 days to 10 years earlier. Table I, which follows, shows the number of employees and non-employees who, respectively, had not logged in to the network for more than 90 days and had never logged in.

Table I

ACS Network Accounts

	Network user accounts	Inactive over 90 days	Never logged in for over 90 days since the account was created
ACS employees	6,161	46	19
Non-ACS employees	5,725	1,801	955
Total network user accounts	11,886	1,847	974

ACS did not properly monitor the level of activity in its user accounts, especially those created for non-employees. ACS stated that it depends on its service providers to validate the identities of their users and that the providers are required to notify ACS when a user account should be created or disabled. However, ACS provided no evidence that it took steps to determine whether its providers adhered to that requirement, such as periodically checking activity levels on their user accounts.

Timely deactivation of user accounts is necessary for the security of private, confidential and sensitive data that exists in ACS network. The continued existence of active user accounts assigned to individuals who are no longer employed by ACS or its service providers creates a vulnerability that could be exploited to compromise the integrity, confidentiality and availability of the agency's critical applications and the data therein. Accordingly, to protect the private information regarding children and families in the ACS network, it is necessary that ACS promptly deactivate the user accounts of individuals who are no longer authorized to access its applications or whose record of inactivity indicates they do not require such access for any authorized purpose. On March 27, 2018, we forwarded the above-described findings to ACS and on May 10, 2018, ACS responded that it will review and disable the inactive accounts.

In addition, we found that the remote access passwords given to the users employed by ACS' contracted service providers never expire, which contravenes DoITT's 90-day password-expiration standard. Passwords that never expire increase the risk of unauthorized access to, and potential exposure of, children's and families' case information. Strong, adequately-enforced controls over access to ACS' applications are essential for the protection of agency computer resources and information. ACS officials stated that they will conduct an audit to recertify the remote users in question, but have not stated whether and how they plan to address the password-expiration requirement.

Recommendations

ACS should:

1. Ensure that all inactive network user accounts are immediately disabled and periodically review user account activity to ensure that only active users and providers have access.

***Agency Response*:** "ACS will strengthen this process. ACS will develop a procedure to validate user accounts every 90 days."

2. Develop and implement a policy requiring regular review of user accounts assigned to service providers to identify and promptly disable inactive accounts.

   Agency Response: "ACS will strengthen this process. ACS will develop a procedure to validate user accounts every 90 days."

3. Develop and implement strong remote-user access policies and procedures, including, but not limited to, a password-expiration policy that complies with DoITT's standards to ensure that only authorized users have access to ACS' network.

   Agency Response: "ACS is working with NYC DoITT to re-design the Juniper remote-access security page to allow login only through the ACS Business Partners link. This will ensure complete compliance with the DoITT password policy for NYC contract-provider users."

   Auditor Comment: We are pleased that ACS is working with DoITT to re-design the remote-access security page. ACS should ensure that the new business link will comply with DoITT's *Password Policy* including the password-expiration standard for remote users.

Inadequate Controls over Administrative and Service Accounts

We found that ACS has insufficient security controls over its administrative and service accounts. Anyone having access to such accounts can make changes to the computer operating system and the system's configuration settings and can create, edit, update and delete user-account information.

To ensure against the improper use of such accounts, DoITT's *Password Policy* states that administrative accounts *should* be, and service accounts *must* be, restricted to logging in from specified Internet Protocol (IP) addresses.[1] However, we found that within ACS' IT environment, such accounts are not restricted to logging in from specified IP addresses. In addition, DoITT's *Password Policy* requires additional security protocols for non-expiring service-account passwords, specifically, that they have a minimum length of 15 characters and be either randomly generated or highly complex.

ACS officials informed us that the passwords of ACS' service accounts, which do not expire, did not meet the DoITT's minimum standards for length and complexity. Without such security controls over its administrative and service accounts, ACS incurs an increased risk of data-breach and the corruption of its data. On May 10, 2018, ACS stated that it will update these passwords to comply with DoITT's *Password Policy*. ACS has not responded to the finding regarding the absence of IP login restrictions.

[1]The IP address provides an identity to each computer using the network.

Recommendation

ACS should:

4. Develop and implement IP login restrictions and password controls for all administrative and service accounts that comply with DoITT's *Password Policy*.

   Agency Response: "ACS will work with NYC DoITT to implement IP-based login requirements. . . . Regarding service accounts, ACS will conduct a full review of service accounts and institute appropriate updated passwords for active accounts."

Lack of Password Controls for Two Applications

Strong password policies are essential controls to protect PII in the computer environment. However, our audit found two of ACS' critical applications that contain sensitive and confidential data, FAF and the Warehouse Inventory Tracking System (WITS), did not comply with DoITT's password standards.[2] DoITT's *Password Policy* states that passwords "must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character. . . . [and] Passwords and PINs must have a minimum length of eight (8) characters." However, we found that WITS users can use passwords that do not comply with those requirements.

DoITT's *Password Policy* also requires that all accounts that provide access to sensitive, private or confidential information "must be automatically disabled after a maximum of 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 policy also states that a password-protected screen lock must be activated within 15 minutes of user inactivity. However, we found that FAF user accounts, which provide access to sensitive and confidential PII, are not disabled after five sequential failed login attempts, and that FAF does not have the DoITT-prescribed password-protected screen-lock feature after 15 minutes of inactivity. We discussed the abovementioned issues with ACS officials and have not received a response to this finding as of the date of this report. Passwords that do not comply with DoITT's standards may be vulnerable to so-called "brute-force attacks," in which unauthorized users attempt to guess the password and thus potentially gain access to the application and the information contained within it.

Recommendations

ACS should:

5. Implement password rules for its WITS system that comply with DoITT's requirements for password length and complexity to prevent and minimize the risk of unauthorized access.

   Agency Response: "ACS is currently working to implement complex password rules for WITS (an older legacy system) to comply with current NYC DoITT password policy. This project should be completed by January 2019."

[2] FAF is used by the DPS Homemaker Unit to perform a standardized assessment of the family that may need services to aid the unit in creating an effective service plan. ACS uses WITS to manage and track the storage of case documentation.

6. Ensure that FAF accounts remain locked for a minimum of 15 minutes after 5 sequential invalid login attempts.

   Agency Response: "ACS is currently working with the FAF vendor to implement these changes to the FAF application. ACS expects completion by January 2019."

7. Implement a timeout feature after 15 minutes of a user's inactivity in the FAF application.

   Agency Response: "ACS is currently working with the FAF vendor to implement these changes to the FAF application. ACS expects completion by January 2019."

Insufficient Access Controls over DPS' Critical Applications

ACS has policies and procedures that limit access to its mission-critical applications that contain private and confidential information. However, our review found that ACS does not properly monitor the user accounts for the FAF and PROMIS applications, which are used by both ACS employees and service providers, to ensure that the agency's policies and procedures are followed.[3]

DoITT's Identity Management Security Policy states that "[u]ser accounts will be created and de-provisioned in a timely manner." ACS is responsible for creating, monitoring and disabling a user's access when the user's employment status changes.

We analyzed ACS' lists of user accounts for DPS' mission-critical applications and found that ACS had not deactivated the accounts of users who had not logged into the two abovementioned applications for more than 90 days. Specifically, 30 of the 74 FAF users (40 percent) had not logged into the application for periods that ranged from over 90 days to 4 years but still had active accounts, according to ACS' list. In addition, 199 of the 2,340 PROMIS users still had active accounts even though they had not logged into the application for periods that ranged from over 90 days to 12 years. Additionally, 177 users listed with active accounts, all associated with contracted service providers, had never logged in since their accounts were created—periods that ranged from over 90 days to 9 years as of the list date. Some of those accounts were created as early as 2009. Further, our field observations found that terminated employees of contracted service providers still had access to PROMIS; their accounts had not been disabled. We forwarded this information to ACS, and ACS stated that it will correct the issue.

Timely deactivation of user accounts is necessary for the security of sensitive data that exists in ACS' applications. The continued existence of active user accounts assigned to individuals who are not or should not be authorized users of its information systems creates a vulnerability that could be exploited to compromise the integrity, confidentiality and availability of the agency's critical applications and the data therein. Accordingly, to protect the City against the risk of unauthorized access to private and confidential information, it is necessary that ACS promptly deactivate the user accounts of individuals who are no longer authorized to access its applications. In that regard, we refer again to Recommendation 2, above, that ACS should develop and implement a policy requiring regular review of user accounts assigned to service

[3] ACS DPS contracted with 60 service providers to perform a variety of services throughout the five boroughs during the period the audit covered. Those service providers are given access to FAF or PROMIS to accomplish their assigned functions. ACS depends on the service providers for authenticating and requesting user accounts for their employees who perform tasks related to ACS-contracted services and for notifying ACS of any changes in their employment status, according to ACS officials.

providers to identify and promptly disable inactive accounts. In addition, we recommend the following two measures.

Recommendations

ACS should:

8. Immediately review and reassess all FAF and PROMIS user accounts to ensure that each user is currently authorized and needs access.

   Agency Response: "PROMIS was reviewed and in full compliance as of May 2018. A script is run nightly in PROMIS to lock all user accounts that have not logged in the past 90 days or not logged in at all. As noted, ACS is currently working with the FAF vendor to implement changes to the FAF applications. ACS expects completion by January 2019."

   Auditor Comment: We are pleased that ACS has reviewed and implemented a PROMIS user account control to lock all users that have not logged in over 90 days or not logged in at all. However, we requested but did not receive documentation showing that a review was conducted and additional controls were implemented.

9. Develop and implement a formal policy and procedure and take any additional steps necessary to ensure that all service providers monitor activity in their assigned user accounts and notify ACS immediately of any changes in their users' employment status and that such notifications result in prompt deactivation of the affected user accounts where warranted.

   Agency Response: "As noted above, a script is run nightly in PROMIS to lock all user accounts that have not logged in the past 90 days or not logged in at all. . . . Moreover, as an additional precaution, there is a quarterly alert in PROMIS when users log on which reminds to update staff. The PROMIS Instructional Guide for Program Directors and Supervisors includes a section detailing how to maintain agency staff information and the PROMIS Help Desk is available to all users. Regarding FAF, as noted, ACS is currently working with the FAF vendor to implement changes to the FAF application. ACS expects completion by January 2019."

   Auditor Comment: In addition to the quarterly alert in PROMIS***,*** ACS should ensure that all service providers will notify ACS immediately of any changes in their users' employment status.

Default Password Weakness

Default passwords for the PROMIS application do not comply with DoITT's *Password Policy*, which states in part that temporary or initial user account passwords and PINs "must be set to expire after initial use." ACS officials informed us that when a new PROMIS user account is created or a password is reset for a service provider's employee, the user needs to obtain a temporary default password from an authorized designee at the service provider's site. However, ACS also informed us that a single default temporary password, which has not been changed for over two years, is shared among all service providers. Continued use and sharing of a common default password among service providers increases the risks of vulnerability to security breaches and unauthorized access. We discussed this issue with ACS officials and recommended that the

agency reassess its practice to comply with DoITT's *Password Policy*. On May 10, 2018, ACS informed us that it will correct this issue by the end of June 2018.

Recommendation

ACS should:

10. Develop a password policy and procedure that requires PROMIS default passwords be changed periodically and comply with DoITT's *Password Policy*.

    Agency Response: "While the Password Policy expresses default password, it does not specifically define how often they should be changed. However, to further enhance the system, ACS will implement a procedure to change the PROMIS default password every 90 days."

Inadequate Data Encryption Policy

We found ACS has insufficient encryption practices for its computer environment. Encryption is a methodology used to protect the confidentiality of data and to significantly reduce the possibility of unauthorized access to agency-critical information. Our audit found that ACS' policy did not require encryption for the data stored in its database and backup tapes residing in ACS data center, both of which contain private, sensitive and confidential information. DoITT's *Encryption Policy* states in part that private or confidential data stored in a database or file system must be encrypted and that removable media including CDs, backup tapes and USB memory drives that contain private or confidential data must be encrypted and stored in a secure location.

After we discussed this issue with ACS officials, they stated that the agency's current policy will be reassessed and modified to implement such controls. Without using the proper data encryption technology, ACS incurs the risk that business-information assets may not receive appropriate protection in the event of theft or accidental loss.

Recommendation

ACS should:

11. Ensure that all private, sensitive and confidential information stored in the database and backup tapes is encrypted.

    Agency Response: "ACS will work to develop and procure updated systems for databases to be encrypted for data-at-rest and for backup tapes. This is a multi-segment/phase project. ACS will be consulting with DoITT. ACS will provide an updated project timeline for the City Comptroller's 90-day follow-up."

Software with Vulnerabilities

According to the *McAfee Vulnerability Manager Report* provided by ACS, the agency uses several outdated operating systems, such as Microsoft Windows Vista, Windows 2000 and Windows Server 2003 that are no longer supported by the manufacturer.[4] Without the necessary security

[4] The McAfee Vulnerability Report Manager is a network scanner that identifies assets (systems) and vulnerabilities in the network. It is also a reporting tool that allows agency to monitor and respond to vulnerabilities.

updates and patches, those products are vulnerable and may allow attackers to gain access to restricted information and to modify, delete and steal data. DoITT's *Vulnerability Management Standard* requires that "[a]ll City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity."

In addition, an ACS *Incident Report* provided to us in January 2018 identified vulnerabilities that required immediate action by ACS. Specifically, the report indicated potential malicious attacks and suspicious activities that required investigation may have occurred.[5] In April 2018, we met with ACS officials to discuss the status of the open and unresolved issues that may lead to security breaches. On May 10, 2018, ACS responded that some of the identified vulnerabilities had been remediated, but it did not provide supporting documentation.

Recommendations

ACS should:

12. Assess and ensure all hardware and software versions are up-to-date.

    Agency Response: "ACS is currently in the process of identifying and remediating non-compliant and end-of–life software."

13. Address and remediate all vulnerability issues and suspicious activities that have been detected.

    Agency Response: "ACS has processes in place to address all NYC Cyber Command Security Operations Center (SOC) related vulnerabilities and associated issues as they arise."

Incorrect User Access Privileges

DoITT's *Identity Management Security Policy* stated that "[a]ccess permissions must be defined in accordance with a user's actual functional work requirements." Under that policy employees should have access privileges to only those functions necessary to perform their job duties. However, contrary to that policy, we found during a PROMIS system demonstration that an ACS staff person could edit case-referral-information detail in a case that was not initiated by or assigned to her. ACS officials informed us that the abovementioned staff person should have read-only access to cases. Currently, ACS is still investigating the cause of the condition we observed.

In addition, we found that PROMIS users have access to certain screens and features that are not within their job functions. Our visits to service providers' sites found providers' caseworkers, supervisors and Management Information System (MIS) staff were given access to the "program monthly notification submission" feature in PROMIS, which provides case statistics and other information to ACS. The service providers' officials informed us that each provider's program director or designated supervisor should be the only individual within each organization submitting the reports in question, once a month, to ACS. Therefore, the providers' caseworkers, MIS staff and non-designated supervisors should not have needed, or have had access to, the abovementioned feature.

[5] The details of the suspicious activities and potential malicious attacks were not included in the report due to the sensitivity of the information and the potential risk associated with the release of such information.

Further, we found that one supervisor employed by a service provider was incorrectly given "administrative assistance" access privileges to PROMIS, which would enable the individual to view, assign and edit *all* cases within the program. The service provider's officials informed us that the individual in question should instead have had access that was limited to only those cases under her supervision. Assigning broad access to a user whose job duties do not require it can expose confidential and sensitive information to unauthorized personnel. Based on our discussions with ACS officials, ACS plans to restrict users from editing any case where they should not have access privileges.

Recommendation

ACS should:

14. Review and ensure that all users are given access to only those features necessary to perform their job duties.

    Agency Response: "ACS gives access as per requirements. ACS can change individual level access as needed. Regarding the demonstration-observation that a staff was able to modify a PROMIS case not assigned to that staff person, ACS immediately reviewed PROMIS and we have remediated the code to ensure that staff cannot change a user entry."

    Auditor Comment: Although ACS stated that user access are given as per requirements, our audit found that service providers had access to PROMIS features that were not needed for their job functions. ACS should communicate with the service providers to require them to reassess their staff's access privileges and ensure that users' access is limited to those features necessary to perform their job duties.

Lack of Disaster Recovery Plan

The City of New York Citywide Application Security Policy mandates that "Application business owners must ensure that each application has a defined Business Continuity Plan and a Disaster Recovery Plan to ensure its readiness to respond to events that could disrupt the application's service continuity." Currently, DoITT is responsible for the backup and disaster recovery of ACS servers that reside in DoITT's data center, and ACS is responsible for backup and disaster recovery for all critical applications and servers hosted in its own data center.

ACS has an overall business continuity plan for its operations; however our audit found that ACS did not have a formal agency-wide disaster recovery plan for its data center. The plan should specify the steps that need to be taken to quickly resume agency operations without material loss of computer data in the event of emergency or system failure. Without such plan, ACS is vulnerable to the loss of critical information and operational ability in the event of a disaster, emergency or system failure.

Recommendation

ACS should:

15. Develop formal agency-wide disaster recovery plan for critical applications that are hosted in the ACS data center.

Agency Response: "ACS will work to update the Disaster Recovery Plan (DR) for critical applications that are hosted in the ACS data center; this project will be completed by January 2019."

Insufficient Physical Security Controls over PII at Service Provider Sites

DPS service providers collect and store physical records containing PII, such as dates of birth, addresses, school records and medical records in their case files. Those files should be kept in locked cabinets and in secured locations. According to the *ACS Records Management Policy for Provider Agencies,* "[p]reventive and foster care agencies are required to maintain their physical (paper) case records in a manner that is consistent with the confidential nature of such records." The policy further states that service providers are required to follow New York State regulations, which state, in part, "[r]ecords containing individually identifiable information shall be marked 'confidential' and kept in locked files or in rooms that are locked when the records are not in use." 18 NYCRR 357.5.

We conducted field visits to 11 randomly selected DPS service providers, out of 60, to determine whether sufficient security controls over the PII the providers collect, store, and dispose of were in place.[6] We found that five service providers stored case files containing PII in unlocked cabinets in open areas that were accessible to the public. In addition, we found PII documentation that had been left in an open recycling bin awaiting pickup and disposal. The PII records exposed through the above-described practices may be at risk of being stolen and misused.

Recommendations

ACS should:

16. Properly store client records in locked secure locations with access limited to only authorized personnel.

    Agency Response: "ACS will be working with the Preventive providers regarding securing and safeguarding client records."

17. Properly secure all PII documentation subject to disposal.

    Agency Response: "ACS will be working with the Preventive providers regarding securing and safeguarding client records."

[6] The 60 DPS service providers included 55 preventive service providers and 5 providers of homemaker services.

DETAILED 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 and 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.

The scope of this audit was from September 2017 to April 2018. We conducted fieldwork from October 2017 to April 2018. To achieve our audit objectives, we:

- Reviewed ACS organizational charts to understand its administration and personnel structures;
- Interviewed various ACS officials from the Division of Preventive Services Unit, Family Home Care Unit, Office of Preventive Family Team Conferencing, Contract Management Unit, Information Technology Unit, PROMIS Unit, Office of Technical Assistance, Community-Based Strategies Unit and Personnel Unit to better understand their daily tasks and operations;
- Conducted system walk-throughs with ACS officials to understand the functionalities of various ACS DPS applications;
- Reviewed NYC Comptroller's Directive #1 to determine whether ACS has proper internal controls; and
- Reviewed contracts and applicable policies between ACS and the DPS service providers to understand the tasks and requirements of the service providers.

To achieve our audit objectives to determine whether ACS has adequate access and security controls to prevent unauthorized access, we:

- Reviewed documentation to determine whether ACS has policies and procedures in place for creating new users and terminating the accounts of inactive users;
- Reviewed the Personnel Unit's policies and procedures to better understand the on-boarding and off-boarding processes for ACS employees;
- Analyzed and reviewed DPS applications to determine whether ACS has adequate access controls to prevent unauthorized access;
- Reviewed ACS password policies to determine whether ACS complies with DoITT's *Identity Management Standard*, *Identity Management Security Policy*, and *Password Policy*;
- Reviewed and analyzed ACS Security Accreditation Documentation for PROMIS to determine whether ACS has adequate controls to ensure proper system operations, data integrity and data confidentiality in PROMIS;
- Conducted password control tests for DPS critical applications such as password format, length and complexity;
- Performed access controls tests for DPS critical applications to determine whether ACS enforces the timeout and lockout features;

- Reviewed and analyzed the ACS' remote access policies to determine whether ACS has sufficient access controls;
- Obtained and reviewed a list of 11,886 network user accounts as of December 20, 2017(external and internal) to determine whether inactive users' access were disabled;
- Compared ACS network users list as of December 20, 2017, to the City's New York City Payroll Management System (PMS) to test whether users who are no longer working for ACS may still inappropriately have access to the network and whether these user access are removed in a timely manner;
- Obtained and analyzed current lists of 2,340 PROMIS users as of December 18, 2017; 74 FAF users as of December 27, 2017; and 332 FTC Database users as of December 21, 2017, to determine whether ACS is actively monitoring its user activities and disabling inactive user accounts;
- Reviewed security policies and procedures to determine whether ACS complies with DoITT's *Encryption Policy* and *Vulnerability Management Policy*;
- Requested ACS backup policies, disaster recovery plan and business contingency plan to ensure ACS has the adequate policies to recover data and continue operations within a reasonable time after disastrous events;
- Conducted data center walkthrough to ensure ACS has adequate physical security to protect its computer environment; and
- Requested and analyzed ACS' internal reports such as threat detection reports, incident reports, McAfee vulnerability manager reports and IBM AppScan to determine whether ACS is actively monitoring its operating systems and applications.

To achieve our audit objectives to determine whether ACS DPS has adequate controls over PII information, we:

- Obtained lists of DPS contracted service providers to determine the number and types of programs and services offered;
- Randomly selected 11 out of 60 DPS service providers to conduct field observations to understand the daily task and operations for collecting PII information;
- Reviewed service providers' access control policies and procedures to determine whether they comply with DoITT standards;
- Requested documentation to determine whether ACS and the service providers are communicating regarding access to ACS computer resources; and
- Conducted field observations to determine whether service providers had proper physical security to safeguard children and families' physical case records.

The results of the above tests, while not projectable to their respective populations, provided a reasonable basis for us to evaluate and support our conclusion about ACS DPS' handling and safeguarding over PII data collected and stored.

Administration for Children's Services

David A. Hansell
Commissioner
150 William Street
New York, NY 10038

Eden Hauslaib
Chief Accountability Officer

Jennifer Fiellman
Assistant Commissioner

June 15, 2018

Marjorie Landa
Deputy Comptroller
City of New York
Office of the Comptroller
1 Centre Street
New York, NY 10007

Dear Ms. Landa:

Thank you for the opportunity to review and comment on the *Audit Report on the NYC Administration for Children's Services' Security Controls Over Its Personally Identifiable Information at the Division of Preventive Services SI18-060A.*

The Administration for Children's Services (ACS) appreciates the review of our older, legacy systems. As discussed with the audit team, ACS works with the New York City Department of Information Technology and Telecommunications (DoITT) and the New York State Office of Children and Family Services (OCFS) in development of new systems and building in compliance with New York City DoITT and New York State OCFS policy at the time of construction.

Our responses to the recommendations follow below.

Recommendation # 1: Ensure that all inactive network user accounts are immediately disabled and periodically review user account activity to ensure that only users and providers have access.

ACS Response to Recommendation # 1
ACS will strengthen this process. ACS will develop a procedure to validate user accounts every 90 days.

Recommendation # 2: Develop and implement a policy requiring regular review of user accounts assigned to service providers to identify and promptly disable user accounts.

ACS Response to Recommendation # 2
ACS will strengthen this process. ACS will develop a procedure to validate user accounts every 90 days.

Recommendation # 3: Develop and implement strong remote-user-access policies and procedures including but not limited to a password expiration policy that compiles with DoITTs standards, to ensure not only authorized users have access to ACS's network.

ACS Response to Recommendation # 3
ACS is working with NYC DoITT to re-design the Juniper remote-access security page to allow login only through the ACS Business Partners link. This will ensure complete compliance with the DoITT password policy for NYC contract-provider users.

Recommendation # 4: Develop and implement IP login and password restrictions for all administrative and service accounts that comply with DoITT's password policy.

ACS Response to Recommendation # 4
ACS will work with NYC DoITT to implement IP-based login requirements. Otherwise, ACS administrative accounts comply with the DoITT Password Policy. ACS administrative accounts are set to expire every 60 days and are not set to "Never Expire." Regarding service accounts, ACS will conduct a full review of service accounts and institute appropriate updated passwords for active accounts.

Recommendation # 5: Implement password rules for its WITS system that comply with DoITT's requirements for password length and complexity to prevent and minimize the risk of unauthorized access.

ACS Response to Recommendation # 5
ACS is currently working to implement complex password rules for WITS (an older legacy system) to comply with current NYC DoITT password policy. This project should be completed by January 2019.

Recommendation # 6: Ensure that FAF accounts remain locked for a minimum of 15 minutes after five sequential invalid login attempts.

ACS Response to Recommendation # 6
ACS is currently working with the FAF vendor to implement these changes to the FAF application. ACS expects completion by January 2019.

Recommendation # 7: Implement a timeout feature after 15 minutes of a user's inactivity in the FAF application.

ACS Response to Recommendation # 7
ACS is currently working with the FAF vendor to implement these changes to the FAF application. ACS expects completion by January 2019.

Recommendation # 8: Immediately review and reassess all FAF and PROMIS user accounts to ensure that each user is currently authorized and needs access.

ACS Response to Recommendation # 8

PROMIS was reviewed and in full compliance as of May 2018. A script is run nightly in PROMIS to lock all user accounts that have not logged in the past 90 days or not logged in at all. As noted, ACS is currently working with the FAF vendor to implement changes to the FAF application. ACS expects completion by January 2019.

Recommendation # 9: Develop and implement a formal policy and procedure and take any additional steps necessary to ensure that all service providers monitor activity in their assigned user accounts and notify ACS immediately of any changes in their users' employment status and that such notifications result in prompt deactivation of the affected user accounts where warranted.

ACS Response Recommendation # 9

As noted above, a script is run nightly in PROMIS to lock all user accounts that have not logged in the past 90 days or not logged in at all. In addition, as discussed with the audit team, contracted agency providers have the ability to deactivate staff from PROMIS; the deactivation function is specifically given to management level staff as cited in the ACS Preventive Standards and Indicators (Staff Qualifications section p. 104). Moreover, as an additional precaution, there is a quarterly alert in PROMIS when users log on which reminds to update staff. The PROMIS Instructional Guide for Program Directors and Supervisors includes a section detailing how to maintain agency staff information and the PROMIS Help Desk is available to all users. Regarding FAF, as noted, ACS is currently working with the FAF vendor to implement changes to the FAF application. ACS expects completion by January 2019.

Recommendation # 10: Develop a password policy and procedure that required PROMIS default passwords be changed periodically and comply with DoITT standards.

ACS Response Recommendation # 10

According to #13 of the DoITT Password Policy, ACS is in full compliance. PROMIS temporary or initial User Account passwords are set to expire after initial use. PROMIS default passwords must be changed immediately upon first login. If a user is not prompted to change a temporary or initial password, they are instructed to send email to acshelp@acs.nyc.gov. While the Password Policy expresses default password, it does not specifically define how often they should be changed. However, to further enhance the system, ACS will implement a procedure to change the PROMIS default password every 90 days.

Recommendation # 11: Ensure that all private, sensitive, and confidential information stored in the database and backup tapes is encrypted.

ACS Response Recommendation # 11

ACS will work to develop and procure updated systems for databases to be encrypted for data-at-rest and for backup tapes. This is a multi-segment/phase project. ACS will be consulting with DoITT. ACS will provide an updated project timeline for the City Comptroller's 90-day follow-up.

Recommendation # 12: Assess and ensure all hardware and software versions are up-to-date.

ACS Response Recommendation # 12
ACS is currently in the process of identifying and remediating non-compliant and end-of-life software. Based on the findings cited by the audit team, ACS validated its environment, and found no instances of Vista or Windows 2000 operating systems. ACS is currently working to upgrade all Windows 2003 server systems; work should be completed on non-legacy systems by January 2019 and legacy systems later in 2019.

Recommendation # 13: Address and remediate all vulnerability issues and suspicious activities that have been detected.

ACS Response Recommendation # 13
ACS has processes in place to address all NYC Cyber Command Security Operations Center (SOC) related vulnerabilities and associated issues as they arise. These processes are documented in prior submissions (Part I and IV) to the audit team.

Recommendation # 14: Review and ensure that all users are given access to only those applications necessary to perform their job duties.

ACS Response Recommendation # 14
ACS gives access as per requirements. ACS can change individual level access as needed. Regarding the demonstration-observation that a staff was able to modify a PROMIS case not assigned to that staff person, ACS immediately reviewed PROMIS and we have remediated the code to ensure that staff cannot change a user entry.

Recommendation # 15: Develop formal agency-wide disaster-recovery plan for critical applications that are hosted in the ACS data center.

ACS Response Recommendation # 15
ACS will work to update the Disaster Recovery Plan (DR) for critical applications that are hosted in the ACS data center; this project will be completed by January 2019.

Recommendation # 16: Properly store client records in locked secure locations with access limited to only authorized personnel.

ACS Response Recommendation #16
ACS will be working with the Preventive providers regarding securing and safeguarding client records. ACS will discuss this in the Provider Bulletin and resend Guidance #2009/11: Records Management Policy for Provider Agencies. ACS will also discuss with providers at the next Quarterly Directors Meeting (July 24, 2018) and distribute SSL 18CRR-NY 357.5: Procedures for Safeguarding Information Maintained by the New York State Department of Social Services.

Recommendation # 17: Properly secure all PII documentation subject to disposal.

ACS Response Recommendation #17
As above, ACS will be working with the Preventive providers regarding securing and safeguarding client records. ACS will discuss in the Provider Bulletin and resend Guidance #2009/11: Records Management Policy for Provider Agencies. ACS will also discuss with providers at the next Quarterly Directors Meeting (July 24, 2018) and distribute SSL 18CRR-NY 357.5: Procedures for Safeguarding Information Maintained by the New York State Department of Social Services.

Thank you for your consideration and for your work in support of New York City's children and families.

Sincerely,

Jennifer Fiellman, Esq.