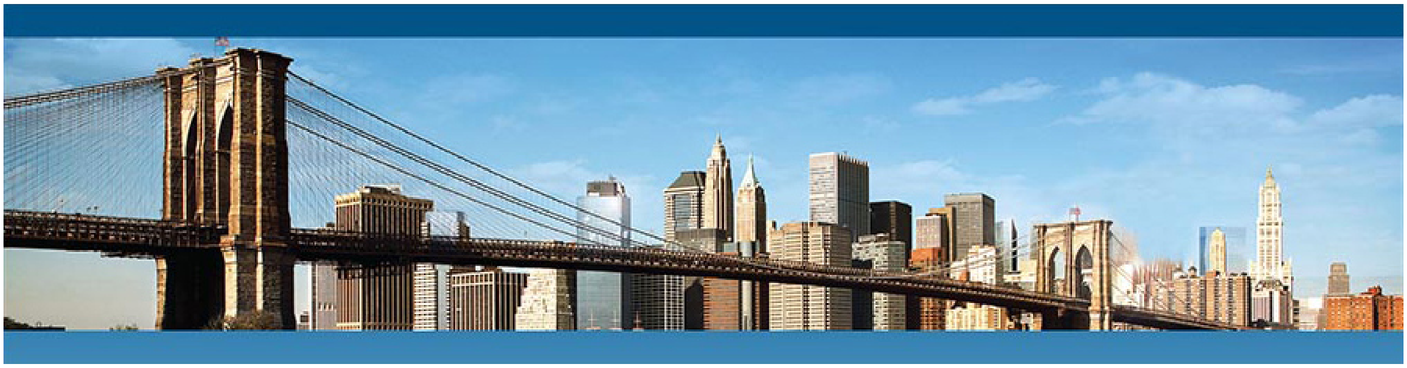
City of New York

OFFICE OF THE COMPTROLLER

Scott M. Stringer
COMPTROLLER



AUDITS AND SPECIAL REPORTS

IT AUDIT

Marjorie Landa
Deputy Comptroller for Audit

Audit Report on the New York City Human Resources Administration's Home Care Services Program's Controls over Personally Identifiable Information

SI18-061A

June 26, 2018

http://comptroller.nyc.gov

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

June 26, 2018

To the Residents of the City of New York:

My office has audited the New York City Human Resources Administration (HRA) Home Care Services Program's (HCSP's) controls over personally identifiable information (PII) to determine whether the HCSP: (1) has adequate controls over the PII that is being collected and stored; and (2) is properly securing personal information from unauthorized access.

The audit determined that although HRA has several information security controls in place, including firewalls and antivirus software to protect its IT systems, physical security for work areas and paper-shredding contracts, the audit found weaknesses in HRA's controls for IT application access, data protection and data classification. As a result, PII is not fully protected in HRA's computerized environment.

Among other issues, the audit found that password functionality controls did not work in two applications. Further, the audit found that HRA did not always implement applicable City password and lockout policies, disable the application user accounts of former and on-leave employees or properly control access to private information for network folder users.

The audit also found that HRA's business continuity and disaster recovery plan needs updating, data classification is incomplete and some hard-copy documentation containing clients' PII was not properly secured while awaiting scanning. Finally, the audit found that HRA needs to promptly address reported vulnerabilities in one of its applications that could allow unauthorized access to restricted information and an agency server.

The audit makes 15 recommendations, including that HRA comply with City password, lockout and account-management policies; ensure that access to the network folder is restricted based on users' defined roles; keep its business continuity and disaster recovery plans up-to-date and tested; and comply with applicable regulations and HRA policy for securing and storing physical documentation that contain PII.

The results of the audit have been discussed with HRA officials, and their comments have been considered in preparing this report. HRA's 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

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

Audit Findings and Conclusions 1

Audit Recommendations 2

Agency Response 2

AUDIT REPORT 3

Background 3

Objectives 4

Scope and Methodology Statement 4

Discussion of Audit Results 4

FINDINGS AND RECOMMENDATIONS 5

Access and Security Control Weaknesses 6

Password Functionality Controls Do Not Work in Two Applications 6

Users Are Not Required to Change Initial Passwords in Two Applications 6

Passwords in One Application Do Not Meet Complexity Requirements 7

Account Not Locked for Prescribed Minimum Length of Time after Five Failed Login Attempts in One Application 7

At Least One Application Does Not Comply with 90-Day Password-Expiration and No-Reuse Rules 8

Potential Unauthorized Access to HRA's Computer Applications through Active User Accounts Assigned to Former and On-leave Employees 9

Inadequately Controlled Access to Network Folder 12

Recommendations 12

Outdated Business Continuity and Disaster Recovery Plan 13

Recommendations 14

Incomplete Data Classification 14

Recommendation 15

PII Documentation Not Physically Secured 15

Recommendation 15

Servers Are Operating with Vulnerabilities 15

Recommendation 16

DETAILED SCOPE AND METHODOLOGY 17

ADDENDUM

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

Audit Report on the New York City Human Resources Administration's Home Care Services Program's Controls over Personally Identifiable Information

SI18-061A

EXECUTIVE SUMMARY

We audited the New York City Human Resources Administration (HRA) Home Care Services Program's (HCSP's) controls over personally identifiable information (PII) to determine whether the HCSP (1) has adequate controls over the PII that is being collected and stored; and (2) is properly securing personal information from unauthorized access.

HRA provides economic support and social services to families and individuals through the administration of various programs, including Cash Assistance, the Supplemental Nutritional Assistance Program, Medicaid, Child Support Services, HIV/AIDS Services, Adult Protective Services, assistance for survivors of domestic violence and Home Care Services, the program covered by this audit.

The HCSP provides access to a variety of Medicaid-funded long-term care programs designed to help eligible elderly or disabled individuals remain safely at home, rather than in a nursing home or other institution. Specifically, the HCSP provides home care services to eligible clients and determines Medicaid eligibility for the clients of New York State's Managed Long Term Care program. To achieve its goal, the HCSP uses several specialized applications to collect, process, store and transmit information, including PII, about its clients.

Audit Findings and Conclusions

Although HRA has several information security controls in place, including firewalls and antivirus software to protect its IT systems, physical security for work areas and paper-shredding contracts, the audit found weaknesses in HRA's controls for IT application access, data protection, and data classification. As a result, PII is not fully protected in HRA's computerized environment.

Among other issues, password functionality controls did not work in two applications, and HRA did not always implement applicable City password and lockout policies, disable the application user accounts of former and on-leave employees or properly control access to private information for network folder users.

The audit also found that HRA's business continuity and disaster recovery plan needs updating, data classification is incomplete and some hard-copy documentation containing clients' PII was not properly secured while awaiting scanning. Finally, HRA needs to promptly address reported vulnerabilities in one of its applications that could allow attackers to gain unauthorized access to restricted information and an agency server.

Audit Recommendations

To address the abovementioned issues, we made 15 recommendations, including that HRA:

- Ensure that its password functionality controls work so that they allow access to its applications to only those users who enter the correct passwords.
- Comply with City password, lockout and account-management policies.
- Immediately disable former and inactive employees' user accounts in all of its applications and thereafter conduct periodic reviews to identify and disable the user accounts of former and inactive employees.
- Deactivate the accounts of any users who have not logged into the applications within the time frames established in the HRA *Account and Password Management Policy*.
- Ensure that access to the network folder is restricted based on users' defined roles.
- Review and update HRA's business continuity and disaster recovery plans to include the current applications.
- Perform the required disaster recovery testing.
- Identify and prepare an alternate site for data processing and communications functions.
- Ensure data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.
- Comply with applicable regulations and HRA policy for securing and storing physical documentation that contain PII.
- Address all detected vulnerabilities by applying the proper patches and configuration changes; a follow-up vulnerability scan report should also be generated to confirm that mitigation of vulnerabilities has taken place.

Agency Response

In its response, HRA generally agreed with 14 of the 15 recommendations and partially agreed with one recommendation.

HRA's written response to the draft report expressed a concern that certain section headings of the draft "g[a]ve the impression" that password controls were lacking generally in the agency rather than in specific aspects of its IT environment, as the report sections themselves made clear. We adjusted the headings to eliminate any such concerns. HRA's additional comments are presented in the relevant sections of this report.

The full text of HRA's response is included as an addendum to this report.

AUDIT REPORT

Background

HRA provides economic support and social services to families and individuals through the administration of various programs, including Cash Assistance, the Supplemental Nutritional Assistance Program, Medicaid, Child Support Services, HIV/AIDS Services, Adult Protective Services, as well as programs for survivors of domestic violence and Home Care Services, the program covered by this audit.

In carrying out its mission for the HCSP, HRA collects, processes, stores and transmits many types of PII regarding its clients. The HCSP provides access to a variety of Medicaid-funded long-term care programs designed to help eligible elderly or disabled individuals remain safely at home, rather than in a nursing home or other institution. Specifically, the HCSP provides home care services to eligible clients and determines Medicaid eligibility for the clients of New York State's Managed Long Term Care program. To achieve its goal, the HCSP uses several specialized applications to collect, process, store and transmit information. Those specialized applications include:

- The Long Term Care Web (LTC Web) for entering, processing and managing HCSP clients' information;
- The Eligibility Data and Image Transfer System (EDITS) for interfacing with the State Welfare Management System (WMS) for eligibility determinations of Public Health Insurance applications;
- The Eligibility Data and Image Transfer System Renewal (EDITS Renewal) for the submission of Public Health Insurance renewal applications;
- The Quality Assurance Tracking Information System (QATIS) for registering any complaints HRA receives about the service providers or home attendants, as well as scheduling and performing unannounced home visits; and
- OneViewer for storing and managing large volumes of scanned images.

The five abovementioned applications contain PII that requires protection, such as clients' names, social security numbers, addresses, dates of birth, diagnoses, prescriptions and financial information. According to the New York City Department of Information Technology and Telecommunications' (DoITT) *Citywide Information Security Policy*, information stored in an agency's applications must 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. HRA is responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment, which includes complying with DoITT's policies and standards.

As the City agency charged with overseeing information technology (IT) and telecommunications for more than 120 City agencies, DoITT provides assistance to help the 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 those policies and standards.

Objectives

The objectives of this audit were to determine whether the HRA HCSP:

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

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 the 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 July 2017 through May 2018. We conducted fieldwork from August 2017 to May 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 HRA officials during and at the conclusion of this audit. A preliminary draft report was sent to HRA and was discussed at an exit conference on May 25, 2018. On June 1, 2018, we submitted a draft report to HRA with a request for comments. We received a written response on June 15, 2018. In its response, HRA generally agreed with 14 of the 15 recommendations and partially agreed with one recommendation.

HRA's written response to the draft report expressed a concern that certain section headings in the draft "g[a]ve the impression" that password controls were lacking in the agency as a whole rather than in specific aspects of its IT environment, as the report narrative makes clear. We revised the headings to eliminate any such concerns. HRA's additional comments are presented in the relevant sections of this report.

The full text of HRA's response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

Although HRA has several information security controls in place, such as firewalls and antivirus software to protect its IT systems, as well as physical security for its work areas and locked bins and shredding contracts for the disposal of papers, the audit found weaknesses in HRA's controls for IT application access, data protection and data classification. As a result, PII is not fully protected in HRA's computerized environment. Specifically, the following control weaknesses were identified:

- Password functionality controls did not work in two applications, where entering random characters in the specific password field allowed access to the application.

- HRA did not always implement and enforce DoITT's initial password-expiration and complexity rules, which are intended to allow only authorized users to gain access to the City's applications.

- HRA did not lock users' access to its systems after a predetermined number of unsuccessful login attempts.

- It appears that at least one HRA application does not comply with DoITT's and HRA's own 90-day password-expiration rules and in effect allowed users to use and reuse their previous passwords indefinitely, a practice that is prohibited by both agencies' password policies and may expose data in the affected application[s] to the risk of unauthorized access.

- User-access had not been disabled for inactive users and former City employees, which could increase security risks.

- HRA workstations did not block access, through the File Explorer application, to clients' information that was stored in the network folder.

The audit also found that HRA's document titled *Business Continuity and Disaster Recovery Plans* is outdated and that three of HRA's applications are not in compliance with DoITT's *Data Classification Policy*, which requires the classification of all data in the agency's IT systems among four categories: public; sensitive; private; and confidential. Moreover, HRA did not physically secure the hard-copy documentation that was stored in its premises until it could be scanned and stored off-site. Finally, HRA has not promptly addressed reported vulnerabilities in one application that could allow attackers to gain unauthorized access to restricted information, modify, delete and steal data, shut down an agency server and affect services.[1]

These matters are discussed in greater detail in the following sections of this report.

[1] National Institute of Standards and Technology (NIST) defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. NIST Special Publication 30 revision 1: Guide for Conducting Risk Assessments.

Access and Security Control Weaknesses

Password Functionality Controls Do Not Work in Two Applications

DoITT's *Password Policy* states that all passwords and personal identification numbers (PINs) used to protect City of New York systems "shall be appropriately configured, periodically changed, and issued for individual use." In accord with that citywide policy, HRA's *Account and Password Management Policy* states that passwords are "an important aspect of computer security in that they are the front line of protection for User accounts. As a result, all access is tracked via a User ID/Password System that limits access to resources associated with that User ID/Password."

However, we found that the password functionality controls in the EDITS and EDITS Renewal applications did not work. Specifically, when we conducted our system tests in EDITS and EDITS Renewal, we observed that rather than requiring the user to enter his or her valid WMS password in the field designated for it, the applications allowed the user to log-in by merely entering *any* characters in the WMS password field. The absence of password functionality controls puts the two applications at risk of unauthorized access that could lead to exposure, theft, modification or deletion of clients' data.

HRA Response: "Users are not required to have a WMS account to access certain EDITS and EDITS Renewal screens and functionality. However, these users have only limited functionality in both applications. Only users with active WMS accounts may access all screens and functionalities, permissible for their user role, and only if they enter their active WMS password. The agency will eliminate the ability to enter random characters in the WMS password field."

Auditor Comment: Although HRA stated that users were not required to have a WMS account to access certain EDITS and EDITS Renewal screens, those applications' password fields should still comply with DoITT's Password Policy to mitigate the risk of unauthorized access to the applications.

Users Are Not Required to Change Initial Passwords in Two Applications

DoITT's *Password Policy* states, in part, "Temporary or initial User Account passwords and PINs must be set to expire after initial use." In accord with that prescription, HRA's *Account and Password Management Policy* states, "All new Users will be assigned a default password by ODSM [HRA's Office of Data Security Management] which must be changed immediately upon first logon."

However, during our system test, we found that in LTC Web, the temporary passwords do not expire after initial use. Once a temporary password is assigned and the user enters it in the application, the user is not required to change it for subsequent logins to that application.[2]

In addition, during our system test, the EDITS Renewal application did not require us to change the EDITS Renewal password assigned to us for our initial login. The EDITS Renewal login screen contains three separate fields for, respectively, (1) the user ID of the person logging-in; (2) the EDITS Renewal password; and (3) the user's WMS password. For our test, the EDITS

[2] LTC Web is a web-based application used by HRA users and providers. To gain access into the application, HRA users have to fill-out a form to request access. Based on the form, the administrator sets up the user profile and user ID. Once access is granted, a temporary password is generated by the system and provided to the user.

Renewal password we were assigned for our initial login was not a temporary password, but one that, according to HRA, (a) remains static, and (b) is assigned to *all* users of the application. (According to HRA, the EDITS Renewal password would always be the same, regardless of the user.) Universal use of a single, shared, unchanging password by multiple users of an application could result in an account being compromised and in unauthorized access to the application and the PII within it.

HRA Response: "The LTC Web and EDITS Renewal legacy applications do not require users to update their password after first logon."

Passwords in One Application Do Not Meet Complexity Requirements

DoITT's *Password Policy* states that passwords and PINs must have a minimum length of eight characters and must contain at least one alphabetic character and at least one numeric character or special character, such as an exclamation point, a number sign, or a dollar sign among others. In addition, HRA's *Account and Password Management Policy* states that passwords "should contain both upper and lower case characters (e.g., a-z, A-Z) and be at least 8 characters long, have digits and punctuation characters as well as letters."

However, we found that the EDITS Renewal password that all HRA users use to access that application did not comply with those complexity requirements, in that it consisted of eight characters that were all of one type. Passwords that do not meet the minimum complexity standards prescribed by DoITT are vulnerable to so called "brute force attack," in which unauthorized users try to guess the password and can potentially gain access to the application and the information it contains.

HRA Response: "EDITS Renewal is a legacy application that is one of the exceptions that will be addressed as part of the phased in upgrading process for legacy systems resulting from the DSS integration."

Account Not Locked for Prescribed Minimum Length of Time after Five Failed Login Attempts in One Application

DoITT's *Password Policy* states 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."

However, HRA's EDITS Renewal application does not comply with the DoITT Password Policy's required minimum lockout-time. During our system test, we entered the wrong password several times into the EDITS Renewal password field. After five failed attempts, we received a message stating, "The account has been locked. Please try again after 3 minutes." A lockout period of 3 minutes, as stated in that "account locked" message, obviously would not comply with DoITT's minimum of 15 minutes. Moreover, even when we entered the correct password in less than the three-minute minimum specified in the message, we were able to login into EDITS Renewal. Hence, the application does not properly lock the account after five failed login attempts. Allowing numerous failed login attempts increases the possibility of an unauthorized user's correctly guessing the password, thus increasing the risk that the personal information collected and stored in the application could be exposed to intruders.

HRA Response: "Password control functionality, including the account locking requirement, at HRA/DSS works in accordance with Citywide policy at the network level and at application level for the majority of applications."

Auditor Comment: This section of the report references HRA's EDITS Renewal application only. When tested, it did not lock the user account for a minimum of 15 minutes after five sequential invalid login attempts as required by DoITT's *Password Policy*.

At Least One Application Does Not Comply with 90-Day Password-Expiration and No-Reuse Rules

DoITT's *Password Policy* states that user account passwords and/or PINS "must expire at least every 90 days," and HRA's *Account and Password Management Policy* states that the authentication mechanisms "will enforce password changes at least every ninety (90) days and enable Users to change their passwords when the account or system is suspected of being compromised."

However, it appears that in at least one application, HRA does not comply with DoITT's and its own 90-day password-expiration rules. During our systems tests, we found that HRA's EDITS Renewal application accepts a universal, unchanging password that HRA assigns to all users. As mentioned above, according to HRA, the EDITS Renewal password would always be the same, regardless of the user.

In addition, because certain requested information—each user's last password change date—was not captured consistently by HRA's LTC Web application, we could not determine whether users of that application are required to change their passwords every 90 days in accordance with the abovementioned policies. However, we did receive that information for the OneViewer user list. Our review of it indicated that five users were able to log-in to the application after their passwords should have expired under the 90-day expiration rules. When we informed HRA officials, they explained that OneViewer users are not required to change their password because their access to that application is based on Active Directory authentication.[3] However, because the agency did not provide us with access to the OneViewer application, and the Active Directory user list provided on May, 7, 2018 could not be verified pending our receipt of information requested from HRA, we could not determine whether OneViewer is compliant with the abovementioned 90-day password-expiration rules.

It should also be noted that DoITT's *Password Policy* states that passwords and PINs "must not be reused for four (4) iterations." Similarly, HRA's *Account and Password Management Policy* states that users "may not be permitted to change their passwords back (re-use) to any of the last four (4) passwords they used in the past." Those no-reuse provisions are intended to complement the 90-day password-expiration rules in both agencies' policies and thereby mitigate the damage that could result from an old password's falling into the wrong hands. However, our tests of the EDITS Renewal application showed that users who opted to change their passwords would be able to reuse their previously-used passwords, contrary to DoITT's and HRA's own "no-reuse" rules.

[3] An "active directory" is a database that keeps track of all the user accounts and passwords in an organization. It allows organizations to store user accounts and passwords in one protected location, improving the organization's security. When a user-account profile is created in any application linked to the "active directory" in the organization's information system, and the user attempts to log into the application, that account is checked, in the background, against the "active directory." Unless the user's ID is active in the "active directory," the user should not be able to login into the application, even if the user's account is active in the application.

To the extent that HRA allows EDITS Renewal users to continuously use a static password to access that application for longer than 90 days, such usage is contrary to DoITT's and HRA's own password policies and defeats their purpose. In permitting the extended use and the reuse of passwords, contrary to applicable policies, HRA incurs an increased risk of unauthorized access into its EDITS Renewal application, which could lead to exposure, theft, modification or deletion of its clients' data. Proper password management serves as a control to protect data security and prevent unauthorized exposure of clients' PII. Conversely, the absence of proper password management increases the risk of such exposure.

HRA Response: "OneViewer is AD authenticated and follows the Citywide password policy, including 90-day expiration requirement. . . .

It is incorrect to state that 'each user's past password change was not captured consistently…' in the legacy LTCWeb application. External remote Juniper users' last login timestamps and last password change dates are captured in AD. Internal users' last login timestamps and last password change dates are captured in the LTCWeb application."

Auditor Comment: As mentioned above, HRA's own user list for its OneViewer application showed that five users were able to log-in to the application after their passwords should have expired under the 90-day expiration rules. HRA did not provide a response that addressed that observation, as requested.

With regard to our observation that each user's last password change date was not captured consistently by HRA's LTC Web application, we requested a list of the application's internal users, including the field that is supposed to show the last date that each user's password was changed. However, according to HRA, the field on the list HRA provided captured either the date the account was first created or, if applicable, the date on which the user selected the "forgot password" option on his or her screen. Because neither of those events necessarily coincides with the date on which the user last changed his or her password, we could not determine, from the information HRA provided, whether users were required to change their LTC Web application passwords every 90 days.

Potential Unauthorized Access to HRA's Computer Applications through Active User Accounts Assigned to Former and On-leave Employees

DoITT's *Identity Management Security Policy* states, in part, "User accounts [should] be created and de-provisioned in a timely manner." However, HRA did not ensure that its user accounts for five applications—LTC Web, EDITS, EDITS Renewal, QATIS and OneViewer—were promptly deactivated for 222 former employees and inactive users, such as employees on long-term leave.[4] HRA is responsible for creating and monitoring access to its applications for its authorized users and for disabling their access when their employment status changes. Its failure to promptly deactivate the user accounts assigned to 222 individuals who either had left agency service or had gone on long-term leave may have exposed its data and that of its clients to the risk of unauthorized access.

We analyzed HRA's lists of active user accounts for the five abovementioned applications as of March 5, 2018, and found that they included a total of 267 active user accounts assigned to 222 former employees or employees on long-term leave. Table I, which follows, shows the numbers

[4] Inactive users may include employees on extended leave, with or without pay, because of factors such as an illness or child care needs, or who are absent from work because of suspension, among other causes.

of active user accounts, by application, assigned to individuals who had previously ended their City-employment status or were on extended leave, according to the City's Payroll Management System (PMS) database.

Table I

Number of Former and On-leave Employees Found in HRA's Active User Account Lists per Application as of March 5, 2018

Application Name	Number of User Accounts	User Accounts Assigned to Former and On-leave Employees
LTC Web	836	12[5]
EDITS	577	47
EDITS Renewal	753	65
QATIS	33	2
OneViewer	968	141
Total User Accounts	**3,167**	**267**
Total Former and On-leave Employees with User Accounts[6]		**222**

Timely deactivation of user accounts is necessary for the security of sensitive data that is stored and accessed through HRA' five applications. The continued existence of active user accounts assigned to individuals who have left HRA—and therefore are not 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 HRA promptly deactivate the user accounts of individuals who are no longer authorized to access its applications.

HRA officials stated at the exit conference that the accounts of 207 of the above-mentioned 222 users had been deactivated in the agency's Active Directory, and therefore those users would not be able to access to the agency's applications. Nevertheless, even if the former and on-leave employees could not personally access the applications, the continued existence of active application accounts in their names poses a risk that those accounts could potentially be exploited by unauthorized users. After the exit conference, HRA submitted an Excel spreadsheet with information and explanations regarding the Active Directory-status of most of the 222 users mentioned above. According to that HRA spreadsheet, 185 of the 222 users' Active Directory accounts were listed as disabled.[7] However, without verifiable supporting documentation, we cannot independently determine whether, or when, the users' accounts were disabled in the Active Directory.

[5] The number excludes five users who were deactivated after we informed HRA of the presence of inactive users on its lists.

[6] The total of user accounts assigned to inactive users in all 5 listed applications is 267. Because an individual user can have access to more than one application, the 267 accounts were assigned to a total of 222 unduplicated users.

[7] HRA provided the following information for the 222 users: 185 users' Active Directory accounts were disabled, 13 were active and Active Directory listings for 10 users were "not found." HRA did not provide information for 14 users.

Moreover, HRA's *Account and Password Management Policy* states that users who have not logged into an application for which they have received a password may have their accounts disabled after specified periods of inactivity—90 days for permanent HRA employees and 30 days for contractors, consultants and temporary employees. However, it appears that HRA did not apply that provision of its own policy. Specifically, in reviewing HRA's lists of active user accounts for the five above mentioned applications, we found 197 HRA users—current or former employees—with a "Last Login Date" value of "Null," meaning they had never logged into the application, and 494 HRA users who had not logged into the applications for 90 days or more. In addition, we found 73 other user accounts, assigned to individuals who may have been contractors, consultants and interns for HRA, with a "Last Login Date" value of "Null," and 221 accounts assigned to users who had not logged into the applications for 30 days or more. Table II, below, shows the numbers of HRA employees, by applications, with active user accounts whose "Last Login Date" value is Null, and "Last Login Date" value is 90 days or more.

Table II

Number of Active User Accounts
with a "Last Login Date" Value of
Null or 90 days or More

Application Name	Total # of User's Last Login Date = NULL	Total # of User's Last Login Date ≥ 90 days
LTC Web	11	66[8]
EDITS	68	175
EDITS Renewal	123	179
QATIS	NA[9]	NA
OneViewer	0	127
Total User Accounts	**202[10]**	**547[11]**
Total HRA Employees	**197**	**494**

We sent the abovementioned user lists to HRA on March 23, 2018 and April 23, 2018, requesting an explanation for why the accounts of users with no login history or with no recent login history—within the preceding 90 days for HRA employees and 30 days for other users—had not been disabled under HRA's *Account and Password Management Policy*. As of the date of this report, HRA has not responded. The presence of users with no recent login history on the lists of active users indicates that the application does not have an activated automatic function to disable users after specified periods of inactivity. Adequate access controls and continual application monitoring—including to identify and eliminate inactive accounts—are necessary to minimize an application's vulnerability to security breaches and the opportunity for the application's misuse.

HRA Response: "HRA provided detailed explanations for the 222 accounts, including information on when accounts were closed and why some remained open. We did not receive any further questions from Comptroller's office after the submission. If data was not sufficient to prove

[8] The number excludes three users who has been deactivated after we informed HRA.

[9] The last login date information was not included in the QATIS user list, and according to HRA, QATIS is tied to the agency Active Directory.

[10] The total number of user accounts with no log-in history ("value of Null") is 202—greater than the total number of HRA employee/users, which is 197—because a user can have access to multiple applications.

[11] The total number of user accounts with the last login date 90 days or longer before the list date is 547, which are assigned to a total of 494 users, as a user can have access to multiple applications.

compliance, we welcome the opportunity to provide additional supporting documents to the auditors."

Auditor Comment: Having been asked since December 2017 to provide the Active Directory list, and having been informed of our finding in March 2018 and in April 2018, HRA provided the abovementioned explanations in regard to the 222 users at the exit conference on May 25, 2018. We informed HRA at that time that we would need supporting documentation by May 29, 2018 to enable us to verify the explanations. On May 29, 2018 HRA provided an Excel spreadsheet with explanations for 208 of the 222 users without the supporting documentation we had requested.

Inadequately Controlled Access to Network Folder

DoITT's *Identity Management Security Policy* states, in part, "Access permissions must be defined in accordance with a user's actual functional work requirements." Similarly, HRA's *Account and Password Management Policy* states, "HRA is compelled . . . to protect Agency/Staff/Client information and to ensure its confidentiality by ensuring that only authorized persons are permitted to access such information."

During our system test, however, we observed that in the workstation provided for testing, we had access to the network folder through the File Explorer application. In the network folder we could access confidential files, one of which contained a folder that contained images with HCSP clients' PII. Not only could we view the content, but we would have been able to make changes to it. Without proper restriction of access, unauthorized users could gain access to certain of the network folder's contents, including clients' information, a breach of the protection that HRA's system should provide. Moreover, unauthorized users would be able to modify the files accessed through the network folder, which could affect the integrity of the data in them. This concern was communicated to HRA, with no response as of the date of this report.

HRA Response: "The majority of agency folders is managed centrally through ODSM and has strict access controls. Folders created by privileged users, notably administrators, do not always follow these rules. HRA is exploring tools that will 'sniff' through the network folders and look for sensitive data and missing access controls. If vulnerabilities are found, we will remediate them immediately. We plan to make recommendation on tool selection by March 2019."

Auditor Comment: HRA should ensure that access to the network folder is restricted based on users' defined roles as required by DoITT's *Identity Management Security Policy* and HRA's *Account and Password Management Policy*.

Recommendations

HRA should:

1. Ensure that its password functionality controls allow access to its applications to only those users that have entered the correct passwords.

   HRA Response: HRA agreed with the recommendation.

2. Ensure that initial passwords are changed immediately upon the first login.

   HRA Response: HRA agreed with the recommendation.

3. Comply with DoITT's *Password Policy* and HRA's *Account and Password Management Policy* to ensure that passwords that provide access to its systems and applications meet the prescribed complexity requirements.

HRA Response: HRA agreed with the recommendation.

4. Ensure that all accounts remain locked for a minimum of 15 minutes to a user who has made five sequential invalid login attempts.

   HRA Response: HRA agreed with the recommendation.

5. Ensure that user account passwords are changed every 90 days.

   HRA Response: HRA agreed with the recommendation.

6. Prevent users from reusing any of the last four passwords they previously used.

   HRA Response: HRA agreed with the recommendation.

7. Immediately disable former and inactive employees' user accounts in all of its applications and thereafter conduct periodic reviews to identify and disable the user accounts of former and inactive employees.

   HRA Response: HRA partially agreed with the recommendation, stating, "Although it is true that the users' application level access was not terminated in this case, at the network level their LAN IDs were terminated timely as part of HRA's daily ceased employee process. Without an active network ID, a user cannot log into our network to access applications."

   Auditor Comment: Even if a former or on-leave employee could not personally access the applications that continued to list him or her, incorrectly, as an active user, the continued existence of such accounts, at the application level, in the names of former and on-leave employees poses a risk that those accounts could potentially be exploited by unauthorized users. Accordingly, we continue to recommend that HRA disable all such accounts.

8. Deactivate the accounts of any users who have not logged into the applications within the time frames established in the HRA *Account and Password Management Policy*.

   HRA Response: HRA agreed with the recommendation.

9. Ensure that access to the network folder is restricted based on users' defined roles.

   HRA Response: HRA agreed with the recommendation.

Outdated Business Continuity and Disaster Recovery Plan

DoITT's *Citywide Application Security Policy* states, in part, "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." Although HRA provided us with a Continuity of Operations Plan (COOP), its business continuity and disaster recovery plan is outdated. The document HRA provided refers to a previous system called Medical Assistance Tracking Information System, which is no longer in production, rather than to the applicable current system, LTC Web. HRA informed us that its document titled *Business Continuity and Disaster Recovery Plans* was last updated in 2007, and the agency is currently updating it. In addition, although the document states that by maintaining and testing the plan, "HRA can be confident that MIS [HRA's Management Information Systems division] will be prepared to resume processing at the recovery facility in a reasonable period after a disaster," HRA did not provide us with any documentation evidencing testing of its plan.

The National Institute of Standards and Technology (NIST) suggests that "[a]lthough major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. . . .[which] should include a strategy to recover and perform system operations at an alternate facility for an extended period."[12] However, the alternate site mentioned in HRA's *Business Continuity and Disaster Recovery Plans* is no longer available. As of April 2018, HRA informed us that it has identified a new alternate site and is waiting for DoITT's recommendation regarding that location. Without an adequate business continuity and disaster recovery plan, proper testing of it, and an alternate site for its data processing and communications equipment and activities, HRA is vulnerable to the loss of critical information and operational ability in the event of a disaster.

Recommendations

HRA should:

10. Review and update HRA's *Business Continuity and Disaster Recovery Plans* to include the current applications.

    HRA Response: HRA agreed with the recommendation.

11. Perform the required Disaster Recovery testing.

    HRA Response: HRA agreed with the recommendation.

12. Identify and prepare an alternate site for data processing and communications functions.

    HRA Response: HRA agreed with the recommendation.

Incomplete Data Classification

DoITT's *Data Classification Policy* states, in part, "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 designate a data steward who is responsible for its data and ensure that its data is labeled appropriately based on the four levels of classification, and that data classified as private and confidential is protected. However, HRA has not provided evidence that it has classified the data in three of its applications as required by DoITT's *Data Classification Policy*. When asked, HRA responded there is no data classification for EDITS and EDITS renewal, and the agency did not provide a response for OneViewer. Without classifying its data in accordance with DoITT's policy, HRA is unable to determine how to adequately protect it, including the PII it contains.

HRA Response: "While data classification is not clearly documented, HRA is applying the strictest available security controls to all categories of data to meet the strictest security requirements, rather than applying controls based on data classification."

Auditor Comment: Without properly documenting and categorizing the data in its applications, HRA cannot ensure that its users would be aware of the sensitivity of the information and how it should be protected and controlled.

[12] Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems.

Recommendation

HRA should:

13. Ensure data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.

    HRA Response: HRA agreed with the recommendation.

PII Documentation Not Physically Secured

New York State Social Services Regulations prescribe procedures for safeguarding information maintained by local social service agencies, such as HRA. The regulation codified at 18 NYCRR 357.5 (a) states, in part, "Records 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." Further, HRA's *Confidentiality Policy* states, "Confidential information should not be left unattended on staff desks or in other unsecured areas of the office. When staff exit their work areas, they must take every precaution not to leave any confidential information where it may be visible or accessible."

During our walkthroughs, we observed several unmarked boxes on top of hallway cabinets and in small unlocked conference rooms that we found contained clients' confidential information. HRA officials stated that the clients' documentation in those boxes still needed to be scanned and that they send such boxes to storage in only after scanning the contents of 150 of them. Although HRA offices have locked cabinets, security guards and locked bins used for disposing/shredding of confidential information, the practice of leaving boxes with clients' confidential information unattended could potentially expose client information to misuse or theft.

Recommendation

HRA should:

14. Comply with applicable regulations and HRA policy for securing and storing physical documentation that contain PII.

    HRA Response: HRA agreed with the recommendation.

Servers Are Operating with Vulnerabilities

According to HRA's vulnerability report for its OneViewer application, the agency had servers operating with 24 unresolved critical vulnerabilities, which include web server vulnerabilities, information disclosure vulnerabilities and denial of service vulnerabilities. Those vulnerabilities could allow attackers to gain access to and execute commands on the servers, which could enable them to gain unauthorized access to restricted information, modify, delete and steal data, shut down the server and affect services.

DoITT's *Vulnerability Management Policy* states, in part, "All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." The policy further states that "[v]ulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the Citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation." Information security is an ongoing process of assessing and addressing security gaps. Open vulnerabilities must be resolved rapidly to prevent attackers from accessing sensitive and confidential information and damaging system operations and data.

Recommendation

HRA should:

15. Address all detected vulnerabilities by applying the proper patches and configuration changes; a follow-up vulnerability scan report should also be generated to confirm that mitigation of vulnerabilities has taken place.

    HRA Response: HRA agreed with the recommendation.

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, 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 the July 2017 through May 2018. We conducted fieldwork from August 2017 to May 2018.

During the planning, survey and review of internal controls phase, we:

- Reviewed DoITT's security policies and standards to determine current security policies in place that apply to City agencies.
- Reviewed HRA's 2016 response to Comptroller's Directive #1, to determine HRA's information technology status and computer environment.
- Reviewed HRA's Fiscal Year 2017 Preliminary Mayor's Management Report to determine the agency's current goals, objectives, and priorities.

During the fieldwork phase, we:

- Reviewed HRA's organization charts to gain an understanding of the agency overall and the units responsible for the administration of the program.
- Conducted walkthroughs of HRA HCSP units, including Medicaid Eligibility Unit, Contracts (Quality Assurance / Contracts Tracking), Field Operations / Community Alternative Systems Agency (CASA), specifically CASA 0, and Manhattan CASA to gain an understanding of how PII is collected and stored and to determine the controls in place to safeguard the applications and data.
- Conducted walkthroughs of the applications (EDITS, EDITS Renewal, OneViewer, and LTC Web) utilized by HRA HCSP to gain an understanding of how users use the applications to conduct their tasks.
- Attended training of LTC Web for service providers to gain an understanding of user needs, information collected, information stored and functions used by providers.
- Conducted meeting with Information Technology Services (ITS) unit to gain an understanding of the architecture of the environments and the controls in place to protect PII.
- Conducted data center walkthrough to gain an understanding of where the data is stored and ensure the physical controls are in place to protect PII data.
- Reviewed user manuals and training documents to gain an understanding the functionality of the applications.

- Conducted field visits to 10 service providers to gain an understanding of the interaction between HRA and providers.[13]
- Requested and reviewed HRA's policies and procedures to gain an understanding of the controls in place safeguarding clients' PII: Confidentiality Policy, Code of Conduct, existing staff, building access, configuration management, security awareness, account and password management, file transfer and remote access.
- Reviewed contracts for the offsite storage of physical documents to gain an understanding of how the data is stored off-site and to ensure it included adequate procedures for properly storing clients' PII.
- Reviewed contracts for the destruction of papers and media and certificates of destruction to ensure it included adequate procedures for properly destroying documents and equipment.
- Reviewed policies, procedures, schedules regarding backup for physical documents and applications to determine whether there are controls in place to support business continuity.
- Requested and reviewed HRA's detailed network diagrams showing critical systems and information security controls to determine the presence of information security controls to safeguard critical systems and data.
- Requested and reviewed HRA's vulnerability AppScan reports for the applications HCSP utilizes to determine the security posture of each application.[14] We requested and reviewed follow-up application vulnerability report to determine whether previously detected vulnerabilities have been addressed.
- Requested and reviewed HRA's vulnerability reports for the HCSP systems to ascertain the weaknesses in the software are fixed and vulnerabilities on the hosts are monitored.[15] Requested a follow-up vulnerability report to determine whether previously detected vulnerabilities have been addressed.
- Requested and reviewed HRA COOP and Business Continuity and Disaster Recovery Plans to determine whether HRA has a continuity plan in place in case of an emergency.

During the fieldwork testing phase, we:

- Requested and analyzed user lists for all of HRA's HCSP applications to determine whether user lists of active staff contain inactive staff that should not have access to the applications. We also tested provided user account lists against City's Payroll Management System.
- Requested and received access to a workstation at HRA location. Performed tests to determine whether adequate security and access controls exist.
- Received a list of service providers and cross-reference to the user list to see whether the users listed were authorized users who belonged to contracted providers.

[13] All City Care / Best Care, All Season Home attendant / Prestige, FEGS Health and Human Services, First Chinese Presbyterian Community Affairs Home Attendant, Hamaspik of Rockland County, Inc., Home Care Service for Independent Living, Pomonok Home Services, Inc., Richmond Home Needs Service, Inc., School Settlement Home Attendant Services Corp., White Glove Community Care.

[14] The IBM Security AppScan 9.0.3 User Guide describes the AppScan application as a security vulnerability testing tool for web applications and web services. It features the most advanced testing methods to help protect site from the threat of cyber-attack, together with a full range of application data output options.

[15] The vulnerability reports were generated by Tenable's Nessus on March 5, 2018 and March 9, 2018 provided by HRA.

- Conducted system tests to determine whether the password functionality controls of the applications used by HRA's HCSP comply with HRA's Password Policy and DoITT's Citywide Information Security Directive and Policies, such as password format, length and complexity. Performed tests to determine whether HRA disables users after five sequential invalid login attempts and has lock-out feature for after 15 minutes of inactivity.

W-2-570
11/17

Department of Social Services

Human Resources Administration

Department of Homeless Services

Office Of Audit & Quality Assurance

Steven Banks
Commissioner

Molly Murphy
DSS First Deputy Commissioner

Saratu Ghartey
Chief Program Accountability Officer

Maria Ciniglio
Deputy Commissioner

150 Greenwich Street
New York, NY 10007

929 221 7126

June 14, 2018

Marjorie Landa
Deputy Comptroller for Audit
New York City Office of the Comptroller
1 Centre Street, room 1100
New York, NY 10007

Re: Agency Response to the Draft Report for the Audit of HRA's Home Care Services Program's Controls over Personally Identifiable Information – SI18-061A

Dear Ms. Landa:

Thank you for sharing with us the Draft Report for the Audit of DHS Oversight of the Human Resources Administration's Home Care Services Program's Controls over Personally Identifiable Information SI18-061A. We have reviewed the referenced report, and our responses are enclosed.

As a threshold matter, we want to emphasize that although we agree with the recommendations put forth in this report, we strongly disagree with the general statement headers in the *Findings and Recommendations* section of the draft report. The general statement headers give the impression that the agency's password controls are lacking, when in reality only a few legacy systems are not currently in compliance with password rules at the application level. It is important to note that on the agency network level we are in compliance with password standards; a user must authenticate their credentials at sign-in before they can attempt to access the individual application. Nevertheless, the agency has prioritized the recommendations put forth in this report and as reflected in our formal response, the majority of the recommendations will be fully implemented by October 2018.

It is also important for the readers of this report to understand the context in which this audit took place. Specifically, that much of the time period being audited occurred while the Human Resources Administration (HRA) and the Department of Homeless Services (DHS) were in the midst of implementing a significant reorganization that resulted in the formation of the Department of Social Services, a new entity which consolidated the administrative functions of both HRA and DHS. Each agency has Administrators who report to the Commissioner of the Department of Social Services. Most administrative functions for both agencies, including contracts and procurement, legal, information technology, program accountability and finance, have been consolidated and serve both agencies. This new structure was implemented following a comprehensive 90-Day Review of DHS operations ordered by Mayor de Blasio that concluded in April 2016. The structural reorganization is significant and is continuing to be implemented.

As part of the reorganization, the Information Technology Services (ITS) is reviewing its processes and structure to identify increased efficiencies and improve service delivery across the agency's large IT portfolio. We have already begun the process of evaluating and prioritizing the necessary systems and data security updates to ensure compliance with City and industry standards. Many of these updates have already been implemented. However, due to the size and depth of our information technology functions, security updates across our applications must be handled in phases, including the few legacy systems that your office audited. We want to assure the Comptroller's Office that we have been and are continuing to prioritize system and security updates in a systematic fashion based on vulnerability and affected client population.

Our mission is to serve New York City's most vulnerable population in the most compassionate, efficient and effective manner, while adhering to all applicable rules, regulations and laws by which we are bound. We would like to express our sincere appreciation for the efforts that your office has invested this review, as it will assist us in achieving our goals. We are confident that our responses demonstrate our commitment to improving our operations going forward. Should you have any questions, please contact me at (929) 221-7126.

Sincerely,

Maria Ciniglio

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
Recommendation 1: HRA should ensure that its password functionality controls allow access to its applications to only those users that have entered the correct passwords.	HRA agrees with the recommendation, but partially disagrees with the underlying findings. The statement "Password Functionality Controls Do Not Work" is incorrect and misleading. Password functionality controls at DSS/HRA work according to the city-wide DoITT policy at the network level, through Active Directory (AD), and at the application level for the majority of applications. The legacy EDITS Renewal application does not rely on AD authentication at present. Users are not required to have a WMS account to access certain EDITS and EDITS Renewal screens and functionality. However, these users have only limited functionality in both applications. Only users with active WMS accounts may access all screens and functionalities, permissible for their user role, and only if they enter their active WMS password. The agency will eliminate the ability to enter random characters in the WMS password field.	**ITS**	Implement Active Directory (AD) authentication for EDITS Renewal. EDITS is already authenticated through AD. Eliminate the ability to enter random characters in the WMS password field in the EDITS and EDITS Renewal logon screens.	**October 2018**
Recommendation 2: HRA should ensure initial passwords are changed immediately upon the first login.	HRA agrees with the recommendation, but partially disagrees with the underlying findings. The statement that "Users Are Not Required to Change Initial Passwords" is misleading and incorrect. On the network level and, in the case of most agency applications, at the application level users are required to change their initial passwords upon first log in.	**ITS**	Implement Active Directory (AD) authentication for LTCWeb and EDITS Renewal.	**October 2018**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
	The LTC Web and EDITS Renewal legacy applications do not require users to update their password after first logon. Once AD authentication is implemented for both applications as part of the phased in upgrading process for legacy systems resulting from the DSS integration, the issue will be remediated.			
Recommendation 3: HRA should comply with DoITT's Password Policy and HRA's Account and Password Management Policy to ensure that passwords that provide access to its systems and applications meet the prescribed complexity requirements.	HRA agrees with the recommendation, but partially disagrees with the underlying findings. The statement that "Passwords Do Not Meet Complexity Requirements" is misleading and incorrect. The HRA/DSS network passwords and those for the majority of agency applications meet DoITT's password complexity requirements. EDITS Renewal is a legacy application that is one of the exceptions that will be addressed as part of the phased in upgrading process for legacy systems resulting from the DSS integration.	**ITS**	Implement Active Directory (AD) authentication for EDITS Renewal.	**October 2018**
Recommendation 4: HRA should ensure that all accounts remain locked for a minimum of 15 minutes to a user who has made five sequential invalid login attempts.	HRA agrees with the recommendation, but partially disagrees with the underlying findings. Password control functionality, including the account locking requirement, at HRA/DSS works in accordance with Citywide policy at the network level and at application level for the majority of applications. Once the AD authentication is implemented for the legacy EDITS Renewal application as part of the phased in upgrading process for legacy systems resulting from the DSS integration, the issue will be remediated.	**ITS**	Implement Active Directory (AD) authentication for EDITS Renewal.	**October 2018**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
Recommendation 5: HRA should ensure that user account passwords are changed every 90 days.	HRA agrees with the recommendation, but partially disagrees with the underlying findings. Password control functionality, including the 90-day expiration rule, works at HRA in accordance with Citywide policy at the network level and at application level for the majority of applications. OneViewer is AD authenticated and follows the Citywide password policy, including 90-day expiration requirement. We would appreciate the opportunity to confirm this for auditor compliance verification. It is incorrect to state that "each user's past password change was not captured consistently…" in the legacy LTCWeb application. External remote Juniper users' last login timestamps and last password change dates are captured in AD. Internal users' last login timestamps and last password change dates are captured in the LTCWeb application. We would appreciate the opportunity to confirm this for auditor compliance verification. Once AD authentication is implemented for EDITS Renewal and LTCWeb as part of the phased in upgrading process for legacy systems resulting from the DSS integration, the 90-days expiration finding will be remediated.	**ITS**	Implement Active Directory (AD) authentication for LTCWeb and EDITS Renewal.	**October 2018**
Recommendation 6:	HRA agrees with the recommendation, but partially disagrees with	**ITS**	Implement Active	**October 2018**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
HRA should prevent users from reusing any of the last four passwords they previously used.	the underlying findings. Password control functionality, including the password reuse rule, works at DSS/HRA in accordance with Citywide policy at the network level and at application level for the majority of agency applications. Once AD authentication is implemented for EDITS Renewal and LTCWeb as part of the phased in upgrading process for legacy systems resulting from the DSS integration, the password reuse finding will be remediated.		Directory (AD) authentication for LTCWeb and EDITS Renewal.	
Recommendation 7: HRA should immediately disable former and inactive employees' user accounts in all of its applications and thereafter conduct periodic reviews to identify and disable the user accounts of former and inactive employees.	HRA partially agrees with the recommendation as well as the underlying findings. Although it is true that the users' application level access was not terminated in this case, at the network level their LAN IDs were terminated timely as part of HRA's daily ceased employee process. Without an active network ID, a user cannot log into our network to access applications. As part of the daily ceased list process, each business day the DSS Personnel department sends an automated email listing all staff that have left the agency a few days prior, either permanently or for a long term leave, to the Office of Data Security (ODSM). ODSM terminates network accounts and WMS accounts, then notifies the Commissioner's office.	**ITS**	Implement Active Directory (AD) authentication for EDITS Renewal and LTC WEB. QATIS, as well as EDITS and One Viewer, are already AD authenticated.	**December 2018**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
	Occasionally terminated accounts are re-activated, typically when termination actions are entered in PMS in error or when the staff member returns from leave. In these cases, the supervisor makes a request to ODSM, and ODSM verifies the accuracy with DSS Personnel before reactivating the LAN ID. Furthermore, ODSM performs monthly verification of the ceased employee process through matches between Active Directory users, WMS users, and PMS employee records. HRA provided detailed explanations for the 222 accounts, including information on when accounts were closed and why some remained open. We did not receive any further questions from Comptroller's office after the submission. If data was not sufficient to prove compliance, we welcome the opportunity to provide additional supporting documents to the auditors.			
Recommendation 8: HRA should deactivate the accounts of any users who have not logged into the applications within the time frames established in the HRA Account and Password Management Policy.	The agency agrees with this recommendation and the underlying findings. The agency currently does not expire accounts after 90 days of non-use for employees and 30 days for consultants. This decision was made to accommodate two user groups where staff do not have to log into work PCs frequently. HRA will explore methods to separate these users so that enforcement can be done for everyone else. We plan to complete this evaluation by end of 2018.	**ODSM & ITS**	Conduct an assessment to identify a protocol that will allow the agency to disable inactive employees after 90 days and consultants after 30 days while allowing the two user groups identified to remain active.	**December 2018**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
Recommendation 9: HRA should ensure that access to the Network folder is restricted based on users' defined roles	HRA agrees with the recommendation, but partially disagree with the underlying findings. The majority of agency folders is managed centrally through ODSM and has strict access controls. Folders created by privileged users, notably administrators, do not always follow these rules. HRA is exploring tools that will "sniff" through the network folders and look for sensitive data and missing access controls. If vulnerabilities are found, we will remediate them immediately. We plan to make recommendation on tool selection by March 2019. In the long term, HRA will review privileged users and ways to better control their ability to create network folders outside of the official process. HRA plans to develop a method by July 2019.	**ODSM & ITS**	Explore tools that will review network folders and look for sensitive data and missing controls. Develop a recommendation to reduce the ability of privileged users to create network folders outside of the official request process.	**March 2019** **July 2019**
Recommendation 10: HRA should review and update HRA's Business Continuity and Disaster Recovery Plans to include the current applications.	The agency agrees with this recommendation. In fact, the HRA COOP Plan is updated on a quarterly basis. The last update to the plan was April 2018. The most updated version of the COOP plan is available to the auditors upon request for compliance purposes. ITS is in the process of updating the entire Disaster Recovery Plan.	**DSS Crisis and Disaster Mgmt and ITS**	Update HRA COOP Plan The DR plans Emergency Contacts Responsibilities, and applications updates to be aligned with current organizational structure	**Completed – April 2018** **December 2018**
Recommendation 11:	HRA agrees with this recommendation.	**DSS Crisis and Disaster**	Review Disaster Recovery Testing.	**Date to be Determined –**

Auditor's Recommendations	Agency Response	Responsible Unit	Agency Corrective Action	Target Date
HRA should perform the required Disaster Recovery testing.	Disaster Recovery Testing will be reviewed. Disaster Recovery Testing is under the auspices of NYC DoITT and the Agency's Crisis and Disaster Unit. Scheduling to be determined pending approval.	**Management / ITS**		**Pending DoITT approval.**
Recommendation 12: HRA should identify and prepare an alternate site for data processing and communications functions.	HRA agrees with this recommendation. ITS Disaster Recovery Alternate site configuration plan has been submitted to NYC DoITT for review. ITS is awaiting approval.	**ITS**	Identify and prepare an alternate site for data processing and communication functions.	**Date to be Determined – Pending DoITT approval.**
Recommendation 13: HRA should ensure data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.	HRA agrees with the recommendation, but partially disagree with the underlying findings. While data classification is not clearly documented, HRA is applying the strictest available security controls to all categories of data to meet the strictest security requirements, rather than applying controls based on data classification.	**ODSM**	Initiate a formal data classification review.	**December 2018**
Recommendation 14: HRA should comply with applicable regulations and HRA policy for securing and storing physical documentation that contain PII.	HRA agrees with this recommendation. HCSP agrees to revise procedures for securing and storing physical documentation that contains PII. Documents containing PII information pending scanning will be secured in locked file cabinets. Scanned documents pending disposal or storage off-site will be secured in a locked file room. Boxed documents containing PII pending pick-up for off-site storage will be secured in a 2nd locked file room.	**HCSP**	Revise and implement procedures for securing and storing physical documentation that contains PII.	**July 2018**

Auditor's Recommendations	**Agency Response**	**Responsible Unit**	**Agency Corrective Action**	**Target Date**
Recommendation 15: HRA should address all detected vulnerabilities by applying the proper patches and configuration changes; a follow-up vulnerability scan report should also be generated to confirm that mitigation of vulnerabilities has taken place	HRA agrees with this recommendation. Almost all applications now reside on Windows 2008 servers. OneViewer application, which accounted for most of the identified vulnerabilities, resided on legacy Microsoft Windows 2003 servers. Given that Windows servers 2003 are no longer supported by Microsoft, there are limitations on the changes we can make to remediate the critical vulnerabilities reported in the Vulnerability scans. Both legacy OneViewer application severs have been taken off of the network by June 7, 2018. As of June 7, 2018, the OneViewer team has completed the process of migrating out of the old infrastructure into two new Windows 2008 R2 servers. Vulnerability scans performed at application level and server level revealed no critical vulnerabilities and only one medium severity vulnerability. Attached are the scanned results. Server scan results and application scan results are available to the auditors upon request for compliance purposes.	**ITS**	Remove two legacy OneViewer application servers from the network. The OneViewer team is in the process of migrating out of the old infrastructure.	**Complete – June 2018**