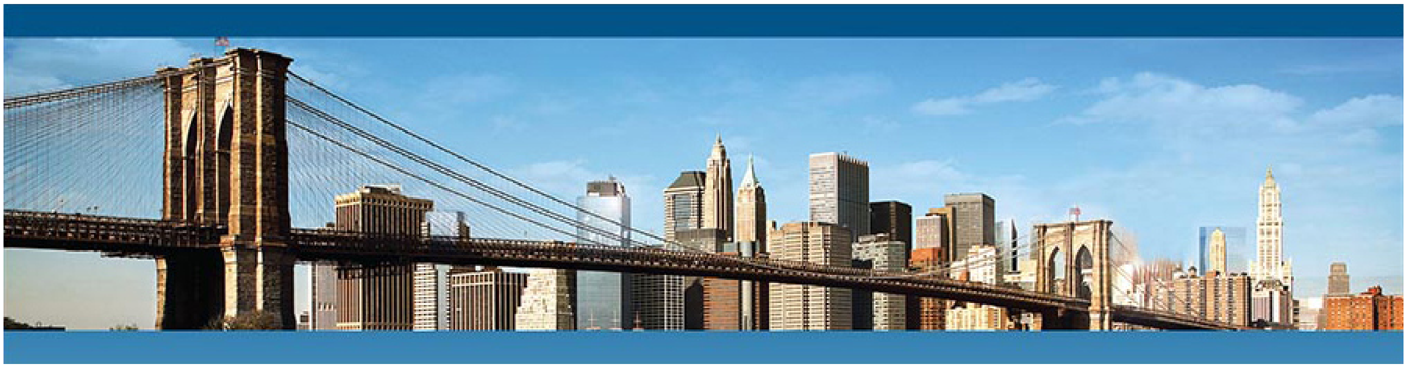
City of New York

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 Department of Parks and Recreation's Access Controls over Its Computer Systems

SI18-087A

June 25, 2018

http://comptroller.nyc.gov

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

June 25, 2018

To the Residents of the City of New York:

My office has audited the New York City Department of Parks and Recreation (DPR) to determine whether it has adequate system security and access controls in place to protect information in its computerized environment. We perform audits of this type of the information technology (IT) systems maintained by City agencies such as DPR 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 DPR has established policies, procedures and guidelines for access control, data protection and security controls to protect information in the agency's computerized environment. However, we found access-control weaknesses, including a failure to disable the accounts of former City employees and inactive users, which could increase security risks. In addition, we found that DPR did not always implement and enforce applicable City password-expiration and complexity rules for its mission-critical applications. Finally, we found that DPR did not have a formal disaster recovery plan for mission-critical applications hosted at its data center.

The audit makes 13 recommendations including that DPR should ensure that all user accounts assigned to former employees and employees on long-term leave are promptly disabled; reassess all current users to ensure that they are given access to only those applications necessary to perform their job duties; ensure that the passwords that provide users with access to its applications meet the complexity standards; and develop a formal disaster recovery plan for DPR applications that are hosted in the DPR data center.

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

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

Sincerely,

Scott M. Stringer

TABLE OF CONTENTS

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

Audit Report on the New York City Department of Parks and Recreation's Access Controls over Its Computer Systems

SI18-087A

EXECUTIVE SUMMARY

This audit was conducted to determine whether the New York City (City) Department of Parks and Recreation (DPR) had adequate system security and access controls in place to protect information in its computerized environment. DPR is responsible for the maintenance of a 30,000-acre municipal park system, which includes most of the City's parks and playgrounds. It also manages forests and trees (both in the parks and on the street), and provides recreational and educational opportunities for New Yorkers of all ages.

To accomplish its varying tasks and conduct its operations, DPR maintains a computer network used by its employees and consultants to access agency emails and files. DPR also maintains several mission-critical computer applications that are accessible to its network users. Many of those mission-critical applications contain sensitive and private information, which includes names, birthdates, addresses, and other information that is intended for agency use only. DPR is responsible for ensuring that it has policies and procedures in place to protect the information in the agency's computerized environment.

Audit Findings and Conclusions

The audit found that DPR has established policies, procedures and guidelines for access control, data protection, and security controls to protect information in the agency's computerized environment. However, we found access-control weaknesses, including a failure to disable the accounts of former City employees and inactive users, which could increase security risks. In addition, DPR did not always implement and enforce applicable City password-expiration and complexity rules for its mission-critical applications. Those rules are intended to allow only authorized users to gain access to City systems.

Further, we found security weaknesses in DPR's computer environment. Specifically, DPR did not perform the required intrusion-detection and vulnerability scans to identify security weaknesses and threats to the servers located in its data center. In addition, DPR did not have a formal disaster recovery plan for mission-critical applications hosted there. Finally, we noted

that the RecWare application DPR uses to manage recreation center memberships and reservations is outdated and no longer supported by the manufacturer. Officials stated that DPR is in the process of replacing RecWare and estimated that the process would take an additional 18 months.

Audit Recommendations

To address the issues raised by this audit, we make 13 recommendations to DPR, including the following:

- Ensure that all user accounts assigned to former employees and employees on long-term leave are promptly disabled.
- Reassess all current users to ensure that they are given access to only those applications necessary to perform their job duties.
- Review and modify current system controls and procedures as needed to ensure that any relevant change in a user's employment status results in prompt deactivation of the user's accounts and periodically conduct reviews to identify and deactivate inactive and unnecessary user accounts.
- Ensure that the passwords that provide users with access to DPR applications meet the complexity standards prescribed by the City Department of Information Technology and Telecommunications (DoITT).
- Ensure that the system that replaces RecWare complies with DoITT's citywide IT security policies, including DoITT's *Password Policy*, to prevent unauthorized access.
- Actively monitor its operating systems and applications to detect and prevent intrusions, periodically perform vulnerability scans, and ensure that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.
- Develop a formal disaster recovery plan for DPR applications that are hosted in the DPR data center and conduct tests to ensure its operational ability in the event of a disaster, emergency, or system failure.
- Promptly resolve the synchronization issue in its tree service application know as FoRMS to ensure that all data is accurate, complete, and consistent.

Agency Response

In its response, DPR stated that with regard to the audit findings concerning access and security weaknesses, it is "implementing corrective measures to ensure enhanced controls moving forward." DPR generally agreed with the audit's 13 recommendations.

AUDIT REPORT

Background

DPR cares for a 30,000-acre municipal park system. The agency specifically maintains the City's parks and playgrounds, manages its forests and trees (both in the parks and on the streets), and provides recreational and educational opportunities for New Yorkers of all ages.

To accomplish its varying tasks and conduct its operations, DPR maintains a computer network used by its employees and consultants to access agency emails and files. DPR also maintains several mission-critical computer applications that are used by its network users.[1] DPR's specialized applications and their uses include:

- The Asset Management Parks System (AMPS), used for maintenance operations;
- The Forestry Management System (FoRMS), used for tracking tree service requests;
- Unifier, used for monitoring capital projects; and
- RecWare, used for managing recreation center memberships and facility reservations.

The four abovementioned mission-critical applications may contain public, sensitive, and private information, which includes names, birthdates, addresses, and other information restricted to agency use.

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 achieve the requisite level of security, adequate access controls such as user-authorization, identification, authentication, access-approval, and login credentials are essential. DPR is responsible for ensuring that it has policies and procedures in place to protect the information in the agency's computerized environment.

As the City agency charged with overseeing IT and telecommunications for more than 120 City agencies, DoITT assists agencies to 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 objective of this audit was to determine whether DPR had adequate system security and access controls in place to protect information in its computerized environment.

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

[1] Mission-critical computer applications are systems that are essential to the agency and failure could result in serious impact on business operations.

audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. 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 October 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 DPR officials during and at the conclusion of this audit. A preliminary draft report was sent to DPR and was discussed at an exit conference held on May 29, 2018. The discussions with DPR officials and the additional information DPR submitted were considered in preparation of the draft report. On June 4, 2018, we submitted a draft report to DPR with request for written comments. We received a written response from DPR on June 18, 2018. In its response, DPR stated that with regard to the audit findings concerning access and security weaknesses, it is “implementing corrective measures to ensure enhanced controls moving forward.” DPR generally agreed with the audit’s 13 recommendations.

The full text of DPR’s response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

The audit found that DPR has established policies, procedures and guidelines for access control, data protection, and security controls to protect information in the agency's computerized environment. However, we found access control weaknesses, including user access that had not been disabled for inactive users and former City employees, which could increase security risks. In addition, DPR did not always implement and enforce DoITT's password-expiration and complexity rules for its mission-critical applications. Those rules are intended to allow only authorized users to gain access to City systems.

Further, we found security weaknesses in DPR's computer environment. Specifically, DPR did not perform the required intrusion-detection and vulnerability scans to identify security weaknesses and threats to the servers located in its data center. In addition, DPR did not have a formal disaster recovery plan for mission-critical applications hosted at its data center. Finally, we noted that RecWare is outdated and no longer supported by the manufacturer. Officials stated that DPR is in the process of replacing RecWare and estimated that the process would take an additional 18 months. These matters are discussed in detail below.

Access Control Weaknesses

DoITT's Identity Management Security Policy states that "[u]ser accounts will be created and de-provisioned in a timely manner." In accord with that citywide policy, DPR is responsible for creating, monitoring, and disabling a user's access when the individual's employment status changes. However, our tests found several access control weaknesses. Specifically, DPR failed to ensure that users' access for former employees and user accounts that remained inactive for over 90 days were promptly deactivated.

Inactive User Accounts Were Not Disabled

DPR has procedures for monitoring user access to its network that include deactivating the accounts of users that have been inactive for over 90 days. However, we analyzed the 5,232 network user accounts DPR listed as current in March 2018 and found that 1,217 (23 percent) of them had been inactive for more than 90 days. Our tests also found that an additional 32 users that DPR listed as having active accounts had never logged into the network since their accounts were created more than 90 days earlier. DPR did not disable the above-described user accounts in a timely manner. Without adequate access controls and continuous monitoring, including timely identification and disabling of inactive accounts, DPR incurs a heightened risk of unauthorized access to its network and the data that can be accessed through it.

In addition, we analyzed the user accounts for DPR's mission-critical applications and found 428 (58 percent) of DPR's 740 RecWare users and 36 (6 percent) of DPR's 567 Unifier users still had access even though they had not logged into the applications for more than 90 days.

On April 27, 2018, we forwarded our lists of inactive users to DPR. DPR officials explained the failure of users to log on for over 90 days by stating that at least some of them may not be required to access the applications in question to accomplish their job responsibilities. However, DPR also stated that it would review and address the abovementioned issues involving inactive user accounts. Without properly validating access permissions in accordance with the user's actual functional work requirements and disabling inactive users promptly, DPR is at risk of someone gaining unauthorized access to its network and agency information.

Former and On-leave Employees Still Had Access to DPR Computer Environment

Timely deactivation of user accounts is necessary for the security of sensitive and private data that exists in DPR's computer environment. In that regard, DoITT's Identity Management Security Policy states that "[u]ser accounts will be created and de-provisioned in a timely manner." However, when we analyzed the list of current network user accounts as of March 23, 2018, and compared it with the City's Payroll Management System (PMS) database, we found that 625 of DPR's 5,232 network users were listed in PMS as former employees or employees on long-term leave. Moreover, 229 of those 625 users had logged into the network *after* they began long-term leave or left DPR's employ.

Based on information DPR reported during and after the exit conference, it appears that 1 of those 229 user accounts is assigned to a former employee who currently is retained as a consultant. However, to properly monitor its network user accounts, DPR should ensure that its lists of authorized users, including consultants, if any, are up to date.

In addition, we analyzed the application-specific user accounts for DPR's mission-critical applications to determine whether they were assigned to active and authorized employees. While RecWare is a single sign-on application, AMPS, FoRMS, and Unifier require two levels of user authentication, i.e. to access each application, each user is required first to log into the DPR network and then to log into the specific application. Table I below shows the number of active users who were listed as retired, terminated, or on leave in the PMS database, but according to DPR's list of active user accounts still had access to the network and four mission-critical applications.

Table I

Number of Former and On-leave Employees Found in Mission-Critical Applications as of January 2018

Mission-Critical Applications	Total Number of User Accounts	Former or On-leave Employees	Former or On-leave Employees with Access to DPR's Network
RecWare	740	268	48
AMPS	1,690	403	103
FoRMS	377	64	19
Unifier	567	14	12

For the protection and security of agency computer resources and information it is necessary that DPR promptly deactivate the user accounts of individuals who are no longer authorized to access its network and applications. The continued existence of active user accounts assigned to individuals who are no longer employed by DPR puts the agency at risk of unauthorized users gaining access to its network and information, which could be exploited to compromise the integrity, confidentiality, and availability of the agency's critical applications and the data therein. DPR officials stated that some of the accounts in question will be deactivated after an internal reassignment of user responsibilities and that some of the accounts have already been disabled after we forwarded the lists to the agency in April 2018. As of the date of this report, however, DPR has not provided us with documentation to support the latter assertion.

Recommendations

DPR should:

1. Ensure that all user accounts for its network and all of its applications that are assigned to former employees and employees on long-term leave are promptly disabled.
2. Reassess all current users to ensure that they are given access to only those applications necessary to perform their job duties.
3. Review and modify current system controls and procedures as needed to ensure that any relevant change in a user's employment status results in prompt deactivation of the user's accounts and periodically conduct reviews to identify and deactivate inactive and unnecessary user accounts.

   DPR Response 1, 2, and 3: "Parks makes every effort to ensure that only its active employees retain access to its computer systems. For example, Parks hires many seasonal employees each year and we work to remove inactive accounts each January when agency headcount activity is at its lowest. The data that the auditors received was from November 2017, prior to the most recent updating. Further, many of the former or on-leave employees cited in the Report as retaining access to Parks' network are employees of Parks' partner organizations and Parks' Information Technology and Telecommunications ('ITT') division is working with those organizations to enhance their intake and removal policies."

   Auditor Comment: In addition to its work to remove inactive user accounts each January, DPR should ensure that the access of former employees, employees on long-term leave, and seasonal employees is promptly deactivated.

Password Control Weaknesses for Two Mission-Critical Applications

The establishment and enforcement of strong password policies are crucial tools that enable DPR to secure its computer environment. However, the audit found that two mission-critical applications, Unifier and RecWare, both of which contain sensitive data, did not comply with DoITT standards. DoITT's *Password Policy* requires the following controls, among others:

- Accounts that provide access to sensitive, private, or confidential information must be automatically disabled after a maximum of 5 sequential invalid attempts within a 15-minute period. After being disabled, the account must remain locked out for 15 minutes.
- User account passwords must expire at least every 90 days, with specific exceptions and conditions for administrative and service accounts.
- Passwords must have a minimum length of eight characters and must not be reused for four iterations.

- Passwords must be constructed using at least one alphabetic character and at least one character that is either numeric or a special character, such as, for example, an exclamation point, a question mark, or a dollar sign, among others.

With respect to DPR's Unifier application, DPR officials stated that the abovementioned DoITT standards can be applied to the application but that they have not yet been enabled by DPR. During the audit, we discussed this matter with DPR officials, and strongly encouraged them to immediately address the deficiency and inform us of any corrective action taken. However, as of the date of this report DPR has provided no information indicating whether such action was taken. In those instances in which its applications are not compliant with the City's password policy, DPR is vulnerable to brute-force attacks in which unauthorized users can guess the password and thus can potentially gain access to the application and the information contained within.

Further, DPR officials stated that RecWare, the other mission-critical application that does not meet DoITT password-control standards, is a legacy system that is no longer supported by the manufacturer and that they intend to replace it. In support of that statement DPR provided the Request for Proposals (RFP) issued on December 15, 2016 to implement a new Recreation/Membership Management system. We discussed the issue with DPR officials and asked DPR to provide us with information regarding the status of the new system's development and implementation.

At the exit conference, DPR officials stated that the agency is in the process of awarding the contract and estimated that once the contract work begins, it will take an additional 18 months to develop and implement the new system.

Recommendations

DPR should:

4. Ensure that the passwords that provide users with access to its applications meet the complexity standards prescribed by DoITT.
5. Ensure that all accounts that provide access to sensitive, private, or confidential information are automatically disabled and remain locked for a minimum of 15 minutes after five sequential invalid login attempts.
6. Prevent users from reusing any of the last four passwords they previously used.
7. Ensure that user account passwords are changed every 90 days.
8. Ensure that the system that replaces RecWare complies with DoITT's citywide IT security policies, including DoITT's *Password Policy*, to prevent unauthorized access.

DPR Response 4, 5, 6, 7 and 8: "Parks is working to ensure that all of its systems meet the complexity standards prescribed by DoITT. The Report found that Unif[i]er and RecWare did not comply with DoITT's *Password Policy*. Parks is in the process of implementing password complexity rules for Unifier that will be consistent with DoITT's policies. RecWare is an older program which did not support password complexity rules and is in the process of being replaced. The contracting and implementation of a new system to replace RecWare is anticipated to take approximately 18 months. The new system is anticipated to comply with DoITT's citywide IT security policies."

Insufficient Intrusion Detection and Vulnerability Scans

DPR's *Incident Management Policy and Response Procedure* states, in part, "Intrusion detection at [DPR] can be divided into internal and external monitoring. [DPR] assumes active responsibility for internal monitoring." However, DPR did not provide supporting documentation to show that it actively monitors agency systems to detect intrusions or performs vulnerability scans to identify security weaknesses and threats to the servers in its data center. The servers located in DPR's data center host AMPS, which is a mission-critical application DPR uses to track work orders, manage storehouse inventory and maintain a centralized property list for the agency.

A vulnerability scan can help analyze, identify, and classify security weakness and threats to an organization's network and applications. According to DoITT's *Vulnerability Management Standard*, "All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." The DoITT standard further states that "[a]t least one agency business unit manager must be assigned who will be responsible for scheduling scans and ensuring that vulnerability tickets are review, remediated, and closed." We discussed this issue with DPR officials, who informed us that, notwithstanding the above-quoted sections of City policies, DPR did not perform intrusion-prevention activities or vulnerability scans. Without periodic vulnerability scans, DPR applications may be at risk of security breaches from internal and external sources.

At the exit conference, DPR officials informed us that DoITT, not DPR, is responsible for vulnerability scans for all DPR servers, notwithstanding the above-quoted provision of DPR's *Incident Management Policy and Response Procedure* which states that DPR is responsible for internal monitoring.

After the exit conference, DPR officials provided emails showing that recently—after the audit identified the issue—DoITT performed vulnerability scans systems that identified security updates and patches that should be installed on DPR's IT systems, which require immediate action. However, DPR did not provide documentation to indicate that the agency has taken the actions that DoITT recommended.

Recommendations

DPR should:

9. Actively monitor its operating systems and applications to detect and prevent intrusions, periodically perform vulnerability scans, and ensure that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.
10. Assign a manager who will be responsible for communicating with DoITT to schedule periodic scans and ensure that vulnerability tickets are reviewed, remediated, and closed.
11. Update its *Incident Management Policy and Response Procedure* to reflect the current procedures that DoITT is responsible for internal and external Intrusion detection and vulnerability scans for all DPR servers.

DPR Response 9, 10, and 11: "Parks' network is completely contained within Citynet, and its servers are inaccessible from public internet. It is not technically possible for a third party vendor to do a remote vulnerability scan. However, ITT will contact NYC Cyber Command and DoITT to determine their recommendations for intrusion detection on Citynet hosted agencies, so that Parks can attempt to meet that standard."

Auditor Comment: Although DPR stated that its servers are inaccessible from the public internet, a potential risk of a security breach from internal and external sources nevertheless exists. Accordingly, vulnerability scans should be performed on a periodic basis and a manager should be assigned to communicate with DoITT.

DPR Lacks a Disaster Recovery Plan

According to DoITT's *Citywide Application Security Policy,* "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 DPR has an overall business continuity plan for its operations, the agency did not have a formal agency-wide disaster recovery plan for its business applications.

Currently, DoITT is responsible for the backup and disaster recovery plan for DPR servers that reside in DoITT's data center. DPR is responsible for backup and disaster recovery for all hardware and software hosted in its own data center. However, DPR officials stated that DPR did not have a formal disaster recovery plan for its data center. DPR should have a plan that specifies the steps that need to be taken to quickly resume agency operations without material loss in the event of a disaster, emergency, or system failure. Without a disaster recovery plan, DPR is vulnerable to the loss of critical information and operational ability should such an event occur.

Recommendation

DPR should:

12. Develop a formal disaster recovery plan for DPR applications that are hosted in the DPR data center and conduct tests to ensure its operational ability in the event of a disaster, emergency, or system failure.

    DPR Response: "Parks is in the process of updating our business continuity plan to include a section on the controls in place for software and hardware in the event of a disaster."

    Auditor Comment: DPR should also develop a formal disaster recovery plan to specify the steps that need to be taken to quickly resume agency operations without material loss.

Other Matter

Data Synchronization and Potential Public Safety Issue Involving FoRMS Tablets

DPR informed us that Panasonic Toughbook tablets are used by its Forestry staff in the field to access FoRMS.[2] These tablets are not given or assigned to specific individuals but rather are

[2] Forestry staff protects and supports the safety and health of the City trees (both in the parks and on the streets).

utilized by multiple staff members to process work orders, perform inspections when needed, and to view, add, or edit information pertaining to tree-service requests. When Forestry staff conducts tree inspections, risk assessments are performed to determine the level of safety of the trees for the public. The tablets enable users to upload data immediately into FoRMS when the Forestry staff is working in the field. During our field visit, we were informed by DPR officials that a small percentage of the data in FoRMS is inaccurate due to a synchronization issue that occurs when the data is uploaded from the tablets into the FoRMS database.[3] DPR officials further stated that some work orders were not transmitted into FoRMS and had to be recreated. DPR reported at the time that it was investigating the potential effects of the discrepancies and seeking a solution for the issue.

At the exit conference, however, DPR officials stated that they are unable to correct the data-synchronization issue but have implemented a new process to track the missing data. Inasmuch as the tree-inspection data in question involves public-safety considerations, an unresolved data-synchronization issue could potentially affect the integrity and reliability of the data within FoRMS that could pose a public-safety risk. Accordingly, DPR should find a permanent solution to resolve the data-synchronization issue and ensure that all tree service requests and work orders are accurately uploaded into FoRMS.

Recommendation

DPR should:

13. Promptly resolve the synchronization issue in FoRMS to ensure that all data is accurate, complete, and consistent.

    DPR Response: "DPR is in the process of replacing Fo[R]MS mobile. While that is in process, the synchronization issue that can cause very few records to need to be re-entered has been supplemented with a fully redundant synchronization process on May 23, 2018 to ensure that all data is preserved. This additional process ensures that no data is lost, missing, or corrupt, and mitigating any potential for a public-safety risk due to synchronization issues."

[3] Synchronization is a process of making two or more data storage devices or programs have exactly the same information at a given time.

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 period of this audit was from October 2017 to May 2018. We conducted fieldwork from December 2017 to May 2018. During the planning, survey, and review of internal controls phase, we:

- Reviewed DPR organizational charts to understand its administration and personnel structures;
- Reviewed DPR's Fiscal Year 2016 Mayor's Management Report to determine the agency's current goals, objectives, and priorities;
- Conducted system walkthroughs with DPR officials to understand the functionalities of various DPR applications; and
- Reviewed New York City Comptroller's Directive #1 to determine whether DPR has proper internal controls.

To achieve our audit objectives in determining whether DPR has adequate system security, we:

- Requested DPR's network diagram to determine the presence of adequate security controls that safeguard DPR systems and data;
- Conducted walkthroughs to ensure DPR has adequate physical security to protect its computer environment;
- Conducted a field observation at a DPR recreation center to assess overall security awareness;
- Requested and reviewed IT operations policy and procedures and backup policy to determine whether DPR has controls in place to support continued system operations;
- Reviewed security policies and procedures to determine whether DPR complies with DoITT's *Encryption Policy* and *Vulnerability Management Policy*; and
- Reviewed DPR's *Parks IT 2017 Continuity of Operations Program* to determine whether the agency has an adequate business continuity plan in place in the event of an emergency.

To achieve our audit objectives in determining whether DPR has access controls in place to protect information in its computerized environment, we:

- Reviewed documentation to determine whether DPR had policies and procedures in place for creating new users and terminating the accounts of inactive users;
- Reviewed DPR password procedures to determine whether DPR complied with DoITT's *Identity Management Standard*, *Identity Management Security Policy*, and *Password Policy*;

- Analyzed and reviewed DPR applications to determine whether DPR has adequate access controls to prevent unauthorized access;
- Conducted tests on password controls such as password format, length, and complexity for DPR mission-critical applications;
- Performed access-controls tests on mission-critical applications to determine whether DPR enforces the timeout and lockout features;
- Compared DPR's network users list as of December 2017 to PMS to test whether users who were no longer working for DPR or on long term leave may have had continuing access inappropriately to the network and whether such users' access was removed in a timely manner;
- Reviewed lists of FoRMS, AMPS, RecWare and Unifier users to determine whether DPR appropriately disabled these inactive users' accounts on its network; and
- Where applicable, the DoITT and/or DPR policies and procedures cited above were used as audit criteria.

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 DPR's access controls over its computer systems.

NYC Parks

Mitchell J. Silver, FAICP
Commissioner

T 212.360.1305
F 212.360.1345

E mitchell.silver@parks.nyc.gov

City of New York
Parks & Recreation

The Arsenal
Central Park
New York, NY 10065
www.nyc.gov/parks

June 18, 2018

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

Re: Draft Audit Report on the New York City Department of Parks and Recreation's Access Controls Over Its Computer Systems (Audit Number SI18-087A)

Dear Deputy Comptroller Landa:

This letter addresses the findings and recommendations contained in the New York City Comptroller's Draft Letter Report ("Report"), dated June 4, 2018, on the above subject matter.

We are pleased that your Report concluded that Parks has established policies, procedures and guidelines for access control, data protection, and security controls to protect information in the agency's computerized environment. With regard to the findings concerning access and security weaknesses, Parks is in the process of implementing corrective measures to ensure enhanced controls moving forward.

In reference to the Report's recommendations to Parks:

Recommendation 1: Ensure that all user accounts for its network and all of its applications that are assigned to former employees and employees on long-term leave are promptly disabled.
Recommendation 2: Reassess all current users to ensure that they are given access to only those applications necessary to perform their job duties.
Recommendation 3: Review and modify current system controls and procedures as needed to ensure that any relevant change in a user's employment status results in prompt deactivation of the user's accounts and periodically conduct reviews to identify and deactivate inactive and unnecessary user accounts.

Parks makes every effort to ensure that only its active employees retain access to its computer systems. For example, Parks hires many seasonal employees each year and we work to remove inactive accounts each January when agency headcount activity is at its lowest. The data that the auditors received was from November 2017, prior to the most recent updating. Further, many of the former or on-leave employees cited in the Report as retaining access to Parks' network are employees of Parks' partner organizations and Parks' Information Technology and Telecommunications ("ITT") division is working with those organizations to enhance their intake and removal policies. ITT has also initiated integration with the Department of Information Technology and Telecommunications' ("DoITT") automatic account deactivation service.

Recommendation 4: Ensure that the passwords that provide users with access to its applications meet the complexity standards prescribed by DoITT.
Recommendation 5: Ensure that all accounts that provide access to sensitive, private, or confidential information are automatically disabled and remain locked for a minimum of 15 minutes after five sequential invalid login attempts.
Recommendation 6: Prevent users from reusing any of the last four passwords they previously used.
Recommendation 7: Ensure that user account passwords are changed every 90 days.

Recommendation 8: Ensure that the system that replaces RecWare complies with DoITT's citywide IT security policies, including DoITT's *Password Policy*, to prevent unauthorized access.

Parks is working to ensure that all of its systems meet the complexity standards prescribed by DoITT. The Report found that Unifer and RecWare did not comply with DoITT's *Password Policy*. Parks is in the process of implementing password complexity rules for Unifier that will be consistent with DoITT's policies. RecWare is an older program which did not support password complexity rules and is in the process of being replaced. The contracting and implementation of a new system to replace RecWare is anticipated to take approximately 18 months. The new system is anticipated to comply with DoITT's citywide IT security policies.

Recommendation 9: Actively monitor its operating systems and applications to detect and prevent intrusions, periodically perform vulnerability scans, and ensure that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.
Recommendation 10: Assign a manager who will be responsible for communicating with DoITT to schedule periodic scans and ensure that vulnerability tickets are reviewed, remediated, and closed.
Recommendation 11: Update its Incident Management Policy and Response Procedure to reflect the current procedures that DoITT is responsible for internal and external intrusion detection and vulnerability scans for all DPR servers.

Parks' network is completely contained within Citynet, and its servers are inaccessible from public internet. It is not technically possible for a third party vendor to do a remote vulnerability scan. However, ITT will contact NYC Cyber Command and DoITT to determine their recommendations for intrusion detection on Citynet hosted agencies, so that Parks can attempt to meet that standard.

Recommendation 12: Develop a formal disaster recovery plan for DPR applications that are hosted in the DPR data center and conduct tests to ensure its operational ability in the event of a disaster, emergency, or system failure.

Parks is in the process of updating our business continuity plan to include a section on the controls in place for software and hardware in the event of a disaster.

Recommendation 13: Promptly resolve the synchronization issue in FoRMS to ensure that all data is accurate, complete, and consistent.

DPR is in the process of replacing ForMS mobile. While that is in process, the synchronization issue that can cause very few records to need to be re-entered has been supplemented with a fully redundant synchronization process on May 23, 2018 to ensure that all data is preserved. This additional process ensures that no data is lost, missing, or corrupt, and mitigating any potential for a public-safety risk due to synchronization issues.

Finally, Parks wishes to thank you and your audit staff for the time and effort devoted to completing this Report.

Sincerely,

Russell Antonucci
Assistant Commissioner for Innovation and Performance Management