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 Department of Design and Construction's Access Controls over Its Computer Systems

SI19-058A

December 20, 2019

https://comptroller.nyc.gov

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

December 20, 2019

To the Residents of the City of New York:

My office has audited the New York City (City) Department of Design and Construction (DDC) to determine whether it has adequate security and access controls in place to protect information in its computer environment. We perform audits of the information technology (IT) systems maintained by City agencies such as DDC to help ensure the security of the data stored in those systems and to minimize the risk of improper access to the City's systems.

The audit found that DDC has established policies, procedures, and guidelines for security and access controls to protect information in its computerized environment. However, we found several weaknesses in certain security and access controls. Specifically, the current DDC data center was constructed over 20 years ago that contains obsolete servers. DDC did not conduct an IT risk assessment to identify security weaknesses and potential threats. The agency failed to promptly remediate vulnerabilities that were identified in the NYC DDC Vulnerability Remediation Reports as needed to mitigate the potential security risks.

In addition, our audit found that user access had not consistently been disabled for inactive user accounts, and for former employees and on-leave employees, which could increase security risks of unauthorized access. We further found that DDC did not maintain accurate user profile information, a lapse that may increase the risk that unauthorized users could gain access to the agency's systems and applications. Finally, DDC failed to comply with Department of Information Technology and Telecommunications' *Password Policy* for one of its critical applications.

The audit makes 17 recommendations, including that DDC should: promptly update and upgrade all outdated software and hardware; perform a periodic risk assessment of all IT assets to evaluate and address all risks associated with its computer environment; immediately address and resolve all vulnerabilities identified; ensure that all inactive network user accounts are immediately disabled; and review all user accounts to ensure the information associated with each user is accurate and current.

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

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

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

SI19-058A

EXECUTIVE SUMMARY

This audit was conducted to determine whether the New York City Department of Design and Construction (DDC) had adequate security and access controls over its computer environment. DDC manages a design and construction portfolio of the City's capital program valued at approximately $13.1 billion. As the City's primary capital construction manager, DDC is responsible for overseeing the construction of many of the City's civic facilities.

In its business operations, DDC uses 43 computer applications, 19 of which the agency identified as critical applications, all of which were reviewed in this audit.[1] DDC's critical applications may contain public, sensitive, private and confidential information, including contract, budget, and payment information. DDC is responsible for ensuring that it has policies and procedures in place to protect the information stored within the agency's computerized environment.

Audit Findings and Conclusions

The audit found that DDC has established policies, procedures, and guidelines for security and access controls to protect information in its computerized environment. However, we found several weaknesses in certain security and access controls. Specifically, DDC maintains obsolete servers that have not been supported by the manufacturer since 2015. Also, the current DDC data center was constructed over 20 years ago and has been deemed "end-of-life."[2] Accordingly, DDC plans to build a new data center and initially informed us that it expected the project to be completed by June 2022. As part of that project, the agency will also assess its current IT infrastructure and replace outdated software and hardware equipment. However, in August 2019, DDC officials informed us that the data center project is on hold and did not provide an estimated timeline to resume and complete the project. In the meantime, DDC's continued use of obsolete hardware and software that are no longer supported by the manufacturers may compromise its

[1] The names and descriptions of the critical applications were not included in the final public version of this report due to the sensitivity of the information and the potential risk associated with the release of such information.
[2] An end-of-life data center contains hardware and software that are no longer manufactured or supported by the manufacturers.

data security and expose the agency to higher maintenance costs and other problems, such as system downtime and business disruption, in its IT-dependent operations.

In addition, DDC did not conduct an IT risk assessment to identify security weaknesses and potential threats. The agency failed to promptly remediate vulnerabilities that were identified in the *NYC DDC Vulnerability Remediation Reports* as needed to mitigate the potential security risks. Furthermore, our audit found that user access had not consistently been disabled for inactive user accounts, and for former employees and on-leave employees, which could increase security risks of unauthorized access to the agency's computerized environment. We further found that DDC did not maintain accurate user profile information, a lapse that may increase the risk that unauthorized users could gain access to the agency’s systems and applications. Finally, DDC failed to comply with Department of Information Technology and Telecommunications’ (DoITT’s) *Password Policy* for one of its critical applications.

Audit Recommendations

To address the abovementioned issues, we made 17 recommendations to DDC, including the following:

- Promptly update and upgrade all outdated software and hardware that had been identified in its data center review.
- Develop a plan to timely address the physical and environmental vulnerabilities at the data center until the relocation is completed.
- Perform a periodic risk assessment of all IT assets to evaluate and address all risks associated with its computer environment.
- Immediately address and resolve all vulnerabilities identified in the 2019 scan reports and obtain a follow-up vulnerability scan report to confirm that the vulnerabilities have been resolved.
- Continue to update the *Continuity of Operations Plan* (COOP) and *Disaster Recovery Plan* to reflect changes in the agency business operations and computer environment.
- Ensure that all inactive network user accounts are immediately disabled and periodically review user account activity to ensure that only active users and providers have access.
- Immediately disable—in its network and critical applications—the user accounts of former employees and employees on long-term leave.
- Review all user accounts to ensure the information associated with each user is accurate and current.

Agency Response

In its response, while DDC addressed each of the audit's recommendations, it did not clearly state whether it agreed or disagreed with them. DDC stated, "In implementing a comprehensive information technology ('IT') strategy, DDC will upgrade legacy project management systems to modern standards and create collaborative tools to empower and link all individuals playing a role in a project." DDC also stated, "DDC is committed to ensuring that there are adequate controls over computer systems and is pleased the auditors recognized that DDC has established policies, procedures and guidelines for security and access controls to protect information in its computerized environment. As it pertains to the findings concerning certain access and security weaknesses, DDC has been and continues to assess its current IT infrastructure as the agency builds out and upgrades its IT."

AUDIT REPORT

Background

DDC manages a design and construction portfolio of the City's capital program valued at approximately $13.1 billion. As the City's primary capital construction manager, DDC is responsible for overseeing the construction of many of the City's civic facilities. It also directly manages the design and construction of civic buildings, such as cultural institutions and libraries. DDC works with other City agencies and with architects and consultants to create and implement design and construction strategies for City construction projects.

In its business operations, DDC uses 43 computer applications, 19 of which the agency identified as critical applications, all of which were reviewed in this audit. DDC's critical applications may contain public, sensitive, private and confidential information, including contract, budget, and payment information.

According to DoITT's *Citywide Information Security Policy*, information stored in an agency's applications must 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. DDC is responsible for ensuring that it has policies and procedures in place to protect the information stored within the agency's computerized environment.

Objective

The objective of this audit was to determine whether DDC had adequate system security and access controls in place to protect information in its computer 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 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 July 2018 through August 2019. 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 DDC officials during and at the conclusion of this audit. A preliminary draft report was sent to DDC officials and was discussed at an exit conference held on November 13, 2019. On November 20, 2019, we submitted a draft report to DDC with a request for written comments. We received a written response from DDC on December 5, 2019. In its response, DDC addressed each of the audit's recommendations.

However, it doing so, it did not clearly state whether it agreed or disagreed with them. DDC stated, “In implementing a comprehensive information technology (‘IT’) strategy, DDC will upgrade legacy project management systems to modern standards and create collaborative tools to empower and link all individuals playing a role in a project.” DDC also stated, “DDC is committed to ensuring that there are adequate controls over computer systems and is pleased the auditors recognized that DDC has established policies, procedures and guidelines for security and access controls to protect information in its computerized environment. As it pertains to the findings concerning certain access and security weaknesses, DDC has been and continues to assess its current IT infrastructure as the agency builds out and upgrades its IT.”

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

FINDINGS AND RECOMMENDATIONS

The audit found that DDC has established policies, procedures, and guidelines for security and access controls to protect information in its computerized environment. However, we found several weaknesses in certain security and access controls. Specifically, DDC maintains obsolete servers that have not been supported by the manufacturer since 2015. Also, the current DDC data center was constructed over 20 years ago and has been deemed "end-of-life." Accordingly, DDC plans to build a new data center and initially informed us that it expected the project to be completed by June 2022. As part of that project, the agency will also assess its current IT infrastructure and replace outdated software and hardware equipment. However, in August 2019, DDC officials informed us that the data center project is on hold and did not provide an estimated timeline to resume and complete the project. In the meantime, DDC's continued use of obsolete hardware and software that are no longer supported by the manufacturers may compromise its data security and expose the agency to higher maintenance costs and other problems, such as system downtime and business disruption, in its IT-dependent operations.

At the exit conference, DDC officials stated that the outdated servers will be decommissioned once the replacement of the legacy applications are completed, but did not provide an estimated timeframe. DDC will also include the data center project as part of its FY 2021 budget plan.

In addition, DDC did not conduct an IT risk assessment to identify security weaknesses and potential threats. The agency failed to promptly remediate vulnerabilities that were identified in the *NYC DDC Vulnerability Remediation Reports* as needed to mitigate the potential security risks. Furthermore, our audit found that user access had not consistently been disabled for inactive user accounts, and for former employees and on-leave employees, which could increase security risks of unauthorized access to the agency's computerized environment. We further found that DDC did not maintain accurate user profile information, a lapse that may increase the risk that unauthorized users could gain access to the agency's systems and applications. Finally, DDC failed to comply with DoITT's *Password Policy* for one of its critical applications.

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

Security Weaknesses

Maintaining effective security controls throughout an organization's computer environment involves an ongoing process of finding and addressing security weaknesses, by actively monitoring the organization's security posture and periodically performing vulnerability scans of its computer environment. However, we found that DDC does not adequately monitor its computer environment and, as a result, we found that it operates with obsolete software in some instances, maintains an outdated data center, did not conduct an IT risk assessment, and failed to remediate vulnerabilities that were identified in the relevant scan reports promptly.

Obsolete Software and End-of-Life Data Center

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." Our audit found that DDC uses outdated software, which is not supported by the manufacturer. We further found that several of DDC's production servers were outdated. Without immediately addressing the need to replace or otherwise stop using these unsupported servers, DDC may be exposed to security risks such as malicious attacks and the loss of electronic data.

When we discussed this issue with DDC officials, they stated that they were aware of it and expected to remediate the vulnerabilities and risks created by the agency's use of the outdated servers in conjunction with the agency's planned new data center project.

According to DDC officials, the current data center was constructed over 20 years ago and has been deemed "end-of-life." The agency had encountered challenges that included constant overheating of the servers and switches housed in the data center, problems with the electrical power supply, and risks of data loss due to the random occurrence of brown-outs at the site. DDC officials stated in substance that over the years some of these problems were addressed individually through piecemeal solutions, such as the installation of commercially available air conditioning units to monitor the temperature and prevent overheating in the data center and uninterruptible power supply units to provide short term power when the electrical power fails.

DDC officials initially stated that they planned to build a new data center to resolve the power and cooling issues and that they expected the project to be completed by June 2022. They also informed us that in conjunction with the data center project, DDC would assess its current IT infrastructure and replace outdated software and hardware equipment. However, in August 2019, DDC officials informed us that the data center project is not part of the current budget plan, and they did not provide an estimated timeline for resuming and completing that project. Without ensuring that its data center is updated and operating more efficiently, particularly, by replacing or discontinuing its use of outdated and unsupported hardware and software, DDC is at risk of compromising the integrity and functionality of its hosted computer environment and may compromise its data security, decrease productivity, incur higher maintenance costs, and be exposed to other problems, such as system downtime and business disruption, associated with non-compliant hardware and software that are no longer supported by the manufacturers.

At the exit conference, DDC officials stated that the outdated servers will be decommissioned once the replacement of the legacy applications are completed, but did not provide an estimated time frame. In the meantime, DDC will continue to work with DoITT to secure the outdated servers. In addition, DDC will include the data center project as part of its FY 2021 budget plan.

Lack of IT Risk Assessment

DoITT's *CISO Role* Policy states that agencies should be continuously "identifying, updating and maintaining information regarding potential security vulnerabilities, risk and threats to the enterprise information technology infrastructure, and distributing technology security information to appropriate staff." We found, however, that DDC has *never* performed a comprehensive agency-wide IT risk assessment to evaluate and address all potential risks associated with its computer environment.

An IT risk assessment is an important and necessary process for any organization that has a responsibility to identify and understand the risks associated with its IT assets and computer environments. An effective risk assessment will define the current agency security posture and cyber vulnerabilities, and provide a plan to mitigate potential risks. An IT risk assessment would assist DDC, for example, in identifying the outdated software and hardware within its computer environment, such as its use of [redacted] and the obsolete equipment in the data center discussed above, and should help the agency reduce the risk of potential threats and prevent attackers from accessing sensitive and confidential information and damaging system operations and data.

Vulnerabilities Were Not Resolved

DoITT's *Vulnerability Management Policy* states, "Agencies must continuously monitor sources of threat and vulnerability information from internal and external security sources." This policy also states, "Agencies must perform a timely review of vulnerability information received from reputable sources." A vulnerability scan can help analyze, identify, and classify security weakness and threats.

DDC officials stated that DoITT and NYC Cyber Command are responsible for conducting vulnerability scans for DDC's computer environment. We analyzed the vulnerability reports based on scans conducted by NYC Cyber Command from February 2019 through May 2019 and found that some of the security weaknesses they identified in DDC's computer environment were not remediated. Specifically, we found that several severe and moderate security risks were identified in consecutive scans in all four monthly scan reports.[3] We requested but did not receive remediation documents that we would need to determine whether any or all of the vulnerabilities identified in these reports had been addressed and resolved.

DoITT's *Vulnerability Management Standard* states, "Scans will open for identified vulnerabilities with severity level 4 or 5, and assign them to the business unit manager. These vulnerability tickets should be resolved and the asset re-scanned within seven days." In this instance, DDC, as the business unit, did not provide us with information indicating whether the required actions were taken.

Without promptly remediating the vulnerabilities identified in the relevant scans, DDC may be at risk of significant security breaches from internal and external sources. DDC may also increase the risk that unauthorized individuals could gain access to restricted information, modify, delete and steal data, and shut down the servers and affect services. Open vulnerabilities must be resolved rapidly to prevent significant security breaches and internal and/or external attackers from accessing sensitive and confidential information and damaging system operations and data.

Inadequate 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."

We reviewed the COOP and *Disaster Recovery Plan* provided by DDC in April 2019 and found that these plans did not sufficiently outline all the administrative and operational procedures needed to ensure that DDC can continue to perform mission-critical functions during and after a disaster. Specially, the *Disaster Recovery Plan* did not include the instructions and actions to be taken in the event of hardware failure, a list of all critical applications, and essential steps that need to be taken to quickly resume agency operations in the event of an emergency or a system failure. A comprehensive plan should include the steps the agency plans to take to mitigate, respond to, and recover from any disruption of its computer operations should an emergency or system failure occur in order to minimize the negative impact and reduce the costs of potential

[3] The details of the vulnerabilities were not included in this audit report due to the sensitivity of the information and the potential risk associated with the release of such information.

loss of data and agency productivity. We discussed the inadequacies of DDC's plans with DDC officials, and they agreed to update the plans.

Accordingly, in August 2019, DDC provided us with its revised COOP and *Disaster Recovery Plan*. DDC officials stated that these plans are marked "draft" and are expected to be updated periodically to reflect changes in DDC's business operations and computer environment. The revised COOP and *Disaster Recovery* plans include a list of the agency's critical applications, actions prescribed for hardware failures, and instructions for resuming agency operations in the event of emergency or system failure. According to the revised *Disaster Recovery Plan*, the agency is expected to perform annual disaster recovery tests, which include simulation and parallel testing at the alternate processing site, to ensure that this plan functions as intended and is adequate to ensure the agency's ability to resume computer operations, restore data quickly, and reduce interruptions in the aftermath of a disaster. We requested but did not receive supporting documentation to show whether DDC had conducted such tests. Without testing the disaster recovery plan, DDC remains vulnerable to the loss of critical information and operational ability in the event of a disaster.

Recommendations

DDC should:

1. Promptly update and upgrade all outdated software and hardware that had been identified in its data center review.
2. Develop a plan to timely address the physical and environmental vulnerabilities at the data center until the relocation is completed.
3. Expedite the new data center project to resolve space, power, and cooling issues.

   DDC Response: DDC responded to recommendations 1, 2, and 3 by stating, "[i]t is not clear what is meant by 'promptly' as DDC complies with the City's procurement rules, which have built in time-periods for each step. Nevertheless, DDC is in the process of building and procuring applications to replace legacy applications. All new applications will be hosted in a cloud- based infrastructure, which will help to mitigate space, power, and cooling issues. An updated request for a new data center will be included in IT's FY2021 budget for approval by DoITT and OMB."

   Auditor Comment: We are pleased that DDC is in the process of building and procuring applications to replace its legacy applications and recognized the need to include the new data center project in its FY 2021 budget plan. However, as noted in the report, DDC is currently operating with obsolete software and hardware that may compromise its data security, IT operations, and could potentially cause business disruptions. These deficiencies should be addressed immediately, and we urge DDC to ensure that actions to do so are expedited in order to minimize the exposure of the security risks and loss of agency data.

4. Perform a periodic risk assessment of all IT assets to evaluate and address all risks associated with its computer environment.

   DDC Response: "Weekly risk assessments are performed by DoITT and these issues are promptly reviewed and remediated by DDC to reduce the risks of potential threats."

Auditor Comment: The weekly scans performed by DoITT are limited to specific components. In fact, DDC has never performed a compressive agency-wide IT risk assessment to analyze, evaluate, and address all potential risks associated with its computer environment. Therefore, we urge DDC to fully implement this recommendation and perform a periodic risk assessment of all IT assets.

5. Immediately address and resolve all vulnerabilities identified in the 2019 scan reports and obtain a follow-up vulnerability scan report to confirm that the vulnerabilities have been resolved.

   DDC Response: "Vulnerabilities discovered in the 2019 scan reports that can be addressed have been addressed. Those that have not been addressed were not addressed because doing so would compromise functionality to the legacy applications that DDC is working to replace. Once the applications are replaced, the vulnerabilities will be reduced."

   Auditor Comment: DDC did not provide supporting documentation that indicated it had reviewed or addressed any vulnerabilities identified in the scan reports. Open vulnerabilities must be reviewed and resolved rapidly to prevent significant security breaches and malicious attacks. DDC should expedite the process to replace all legacy applications and vulnerabilities that are related to these applications should be closely monitored. Therefore, we urge DDC to implement this recommendation and maintain the necessary documentation to memorialize what it did.

6. Ensure periodic vulnerability scans are conducted, reviewed and promptly resolved to reduce the risks of potential threats.

   DDC Response: "Vulnerability scans are conducted weekly and potential threats are discussed and remediated or addressed. Resources for which we cannot apply the recommended remedies are continually monitored and backed-up to reduce the risk of data loss or functional degradation."

   Auditor Comment: DDC did not provide documentation to support its assertions that any of the vulnerabilities were reviewed, addressed or remediated periodically. Therefore, we urge DDC to implement this recommendation and maintain the necessary documentation to memorialize what it did.

7. Continue to update the COOP and *Disaster Recovery Plan* to reflect changes in the agency business operations and computer environment.

8. Periodically conduct tests of the COOP and disaster recovery plans to ensure the agency's operational ability in the event of a disaster, emergency or system failure.

   DDC Response: DDC responded to recommendations 7 and 8 by stating, "DDC does this already and will continue to update the COOP and Disaster Recovery Plan as necessary and periodic tests will be conducted as outlined in the plans."

Access Control Weaknesses

DDC has established access control policies and procedures for protecting its computer environment. However, we found several access control weaknesses. Specifically, inactive user accounts were not disabled and former and on-leave employees still had access to the agency's applications and network. In addition, DDC failed to comply with DoITT's *Password Policy* for one of its critical applications, and the network user account contained incorrect information.

Inactive User Accounts Were Not Disabled

DoITT's *Identity Management Security Policy* states, "User accounts will be created and de-provisioned in a timely manner." DDC has a policy for monitoring user access to its network that includes a procedure to disable all user accounts that have been inactive for over 60 days. Although DDC disables inactive user accounts, we found that DDC failed to consistently enforce its own procedure. Our analysis of 1,779 network user accounts listed as active as of December 24, 2018 found that 135 of them had been inactive for periods ranging from 61 days to 648 days and would still provide the users with access to the DDC network. Without adequate access controls and continuous monitoring, including the prompt identification and disabling of inactive accounts, DDC incurs a heightened risk of unauthorized access to its network and the data that can be accessed through it.

Former and On-leave Employees Still Had Access to DDC's Computer Environment

Timely deactivation of user accounts is necessary for the security of sensitive and private data that exists in DDC's computer environment. In that regard, DoITT's *Identity Management Security Policy* states, "User accounts will be created and de-provisioned in a timely manner." When we analyzed DDC's list of current network users and compared it with the City's Payroll Management System (PMS) database, however, we found that 83 individuals listed as active network users were listed in PMS as former employees or employees on long-term leave. Without disabling the access of former employees whose employment with DDC has been terminated and employees on long-term leave, DDC increases the risk of unauthorized access to its network and applications that could lead to exposure, theft, modification, or deletion of its data.

In addition, we found that the accounts for 25 of those 83 former employees or employees on long-term leave had been used to log into the network after the individuals left DDC or began long-term leave. For example, one user account was used to log into the network nine years after the employee-user had ceased working for DDC, according to the PMS record. We discussed this issue with DDC officials, who stated that some of those 25 accounts were accessed and used by other authorized staff to retrieve information by special request. However, DDC officials did not provide supporting documentation for that assertion.

Without continual monitoring of its users' access, DDC may increase the risks of security breaches and the opportunity for the misuse of its systems and data.

Critical Application Access Control Weaknesses

DoITT's *Identity Management Security Policy* states, "Users must be positively and individually identified and validated prior to being permitted access to any City computing resource. . . . [and] will be authenticated at a level commensurate to the data classification of the information being accessed. . . . Access permissions must be defined in accordance with a user's actual functional work requirements." Some of DDC's 19 critical applications are configured to authenticate user accounts through the Windows Active Directory (AD).[4] We analyzed the user lists for those critical applications and compared them against the AD user list, including DDC employees, consultants, interns and external users, to verify whether these user accounts were assigned to valid users.

[4] The Active Directory is essentially a database that keeps tracks of an organization's resources (i.e., users, computers, and printers). One of its functions is to provide centralized authentication and authorization.

We were unable to verify 50 user accounts that were listed as active in DDC's [redacted] application, one of its 19 critical applications, but not on the agency's AD list—an inconsistency. These 50 users were identified in the [redacted] user list as consultants who had access to project related financial data in [redacted]. We forwarded the issue to DDC officials, who did not respond with an explanation for why these consultants' accounts were active according to the [redacted] list but were not included in or were missing from the AD.

In addition, we found that 112 [redacted] users' accounts had been disabled in the AD, indicating that the users should no longer have access to DDC's computer environment, but were still listed as active in the [redacted] application. We forward the list to DDC officials, who responded by stating that because these accounts had been deactivated in the AD the users would not be able to access the [redacted], notwithstanding that their accounts continued to be listed as active in that application. Further, DDC officials responded that they would reassess the agency's current policy to develop new processes to eliminate this issue in the future.

The continued existence of user accounts assigned to individuals whose authorization to use the applications has ended or cannot be verified as current increases the risk of unauthorized access to DDC's applications data and potential exposure or loss of its sensitive information.

Incorrect User Account Information

DoITT's *Identity Management Security Policy* states, in part, "Users must be positively and individually identified and validated prior to being permitted access to any City computing resource." In accordance with that requirement, DDC includes in its AD account information each user's unique Employee Reference Number (ERN), which serves as a verification number, and should signify that the user is a specific, identifiable City employee. However, DDC did not maintain accurate user profile information in assigning and maintaining user accounts for its employees. Specifically, we found that 6 ERNs were assigned to 20 users (one ERN was erroneously assigned to ten different AD users, and five ERNs were erroneously assigned to two users each). We forwarded and discussed the issue with DDC officials, who then found that the problem was caused by system errors and stated that they would review and address this issue.

In addition, we could not verify the employment status for seven users who had wrong ERNs assigned to their accounts. We forwarded the issue to DDC officials who responded that they would review and address it. Without maintaining accurate user information, DDC may be at risk of granting access to its computer environment to unauthorized users who potentially could modify or delete data, or perform other malicious activities.

At the exit conference, DDC officials stated that they will work with DoITT to resolve the wrong ERN issue.

Inadequate Oversight of User Accounts

DoITT's *Identity Management Security Policy* states, "User accounts will be created and de-provisioned in a timely manner." DDC's corresponding process requires the agency's Human Resource Division to notify DDC's Information Technology Services (ITS) office to create and disable user access as employees join and leave the agency. As part of that process, DDC uses [redacted] System [redacted] to process personnel actions, new hires, and separations.

Based on the AD user list and 91 [redacted] new user account request notifications provided by DDC in December 2018, we found that 39 user accounts were created prior the [redacted] notifications. We forwarded the issue to DDC officials, who responded that these [redacted] notifications were generated when employees who were previously or already employed with DDC returned to work after being away on leave or changed titles. Based on their preexisting DDC employment, these 39 employees' user accounts already existed in the network, and their access was enabled when DDC's ITS office received the [redacted] notifications. We noted, however, the notifications were automatically generated as new hire messages rather than as messages relating to changes in the users' preexisting employment status. ITS officials also stated that they do not receive an [redacted] notification when an employee leaves the agency or is placed on long-term leave or inactive payroll status. The ITS office is in the process of updating the [redacted] system to address these issues. In the meantime, ITS officials informed us, [redacted] and AD will be periodically reconciled manually.

In addition, we found that 64 network user accounts were created without evidence of the corresponding [redacted] notifications. According to DDC officials, these accounts were created prior the [redacted] notification because a lengthy onboarding process delayed the latter and the individuals were working and needed access to DDC's information systems before the process was formally completed. However, DDC did not provide any evidence to justify the creation of these accounts. Without proper documentation for tracking user account requests, DDC may be at risk of granting access to users that are not authorized to access the agency's sensitive and private information.

One Critical Application Did Not Comply with DoITT's *Password Policy*

We found that one critical application [redacted] did not comply with DoITT's *Password Policy*, which specifically requires that passwords:

- Must have a minimum length of eight (8) characters.
- Must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character.
- Must be automatically disabled after a maximum of five (5) sequential invalid attempts within a fifteen (15) minute period. After being disabled, account must remain locked out for fifteen (15) minutes.

Our tests found that [redacted] allows only one digit or one character as an acceptable password and did not automatically disable user access after more than 20 failed login attempts. We also found that the user's initial password for [redacted] does not expire as mandated by the DoITT standard.

We discussed these password control weaknesses with DDC officials, who stated that [redacted] is a legacy system. DDC does not plan to implement the DoITT-prescribed password controls in [redacted] and instead plans to replace [redacted] functionalities with other applications in June 2020. Notwithstanding those plans, however, in the absence of effective password controls, unauthorized users could potentially guess the password and gain access to this critical application. Accordingly, we strongly urge DDC officials to immediately develop a temporary solution to address these control weaknesses for as long as the application remains in use.

At the exit conference, DDC officials stated that they are planning to replace [redacted]. Therefore, they will not implement the password policy.

Recommendations

DDC should:

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

   DDC Response: "All accounts, which includes employees, consultants and interns are being disabled through multiple sources. A nightly script will automatically disable users that HR changes to inactive status. Separation reports are sent when a user's effective end date is entered into the Active Directory ('AD') to cease the account. Additionally, accounts are automatically ceased after 90 days of inactivity per DoITT's policy."

10. Enforce the policy of disabling user accounts that have not been used to log into the system in over 60 days.

11. Immediately disable—in its network and critical applications—the user accounts of former employees and employees on long-term leave.

    DDC Response: DDC responded to recommendations 10 and 11 by stating, "DDC makes every effort to ensure that only its active employees retain access to its computer systems. In accordance with DoITT's policy for City agencies, DDC currently has a 90-day policy for disabling user accounts that have not been logged into."

    Auditor Comment: We are pleased that DDC has a 90-day policy for disabling user accounts that have not been logged into its computer systems.[5] However, DDC should immediately disable user access for all former employees and employees on long-term leave.

12. Review and reassess all [redacted] user accounts to ensure that each user is currently authorized and needs access.

    DDC Response: "[redacted] does not contain sensitive information and all active AD users are authorized to have access to view the information contained within [redacted]."

    Auditor Comment: Regardless of the information residing in [redacted], proper access controls to any applications should be limited to authorized users only. Therefore, we urge DDC to properly review and reassess all [redacted] user accounts.

13. Immediately investigate the instances of users with the wrong ERNs, including the assignment of what should be unique ERNs to multiple users, to reduce the risk of granting access to users who are not authorized to have it.

14. Review all user accounts to ensure the information associated with each user is accurate and current.

15. Ensure that accounts are created only for authorized users and that all account creations are properly documented.

    DDC Response 13, 14, and 15: "DDC will continue to monitor for and investigate instances of users with incorrect ERNs and review user accounts to ensure they

[5] DDC amended its policy from 60 days to 90 days to be consistent with DoITT's policy.

are authorized, and that information associated with the account is accurate and current. ERNs are not assigned by DDC and errors with numbers are generally due to a scripting issue at DoITT. DDC provides ticket numbers for these instances so that DoITT will work to resolve issues resulting from their script."

Auditor Comment: We are pleased that DDC will address the incorrect ERNs issue with DoITT. However, DDC's response did not address recommendation 15. As stated in the audit report, we found 64 network user accounts were created without evidence of the corresponding notifications. Therefore, we strongly recommend that DDC implement this recommendation.

16. Promptly upgrade the [redacted] system to ensure its ability and consistent use to send proper, accurate notifications of all relevant personnel actions to timely create and disable user accounts in accordance with applicable City policies.

    DDC Response: "DDC's [redacted] system does not adequately meet the functionality requirements of sending notifications to IT. As a result, DDC's HR personnel has implemented a separation personnel procedure which promptly provides e-mail notifications of all relevant personnel actions to DDC's IT to ensure the timely creation and disabling of user accounts. DDC's IT has an assigned manager who is responsible for ensuring that user accounts are created and disabled in accordance with the applicable City policies."

    Auditor Comment: Although DDC has implemented a procedure for creating and disabling user accounts, it should reassess or upgrade the [redacted] system to meet the functionality requirements of sending notifications to IT.

17. Implement password rules for [redacted] to comply with DoITT's *Password Policy* to prevent and minimize the risk of unauthorized access.

    DDC Response: "Passwords entered into [redacted], which is in the process of being phased out, are secondary and not subject to the policy because a user must be logged into AD in order to gain access. Active Directory password requirements comply with the complexity standard of DoITT's Password Policy to prevent unauthorized access."

    Auditor Comment: This is a Web-based application that users can gain access to without logging into their AD accounts. At the exit conference, we informed DDC official that our AD account was inactive over 90 days and we were still able to access [redacted] successfully through the internet by using the unexpired one digit password. Therefore, we urge DDC to implement this 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 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 July 2018 through August 2019. To achieve the audit objectives, we reviewed pertinent documentation (listed under bullet-points below), conducted system walkthroughs, and performed system testing.

To understand DDC's business process, functions and operations, we:

- Reviewed DDC's organizational charts to understand its administration and personnel structures;
- Reviewed DDC's Fiscal Year 2018 Mayor's Management Report to determine agency's current goals, objectives, resources, and priorities;
- Reviewed DDC's New York City Comptroller's Directive #1 for Calendar Year 2017 and 2018 checklists as part of our effort to determine whether DDC has adequate internal controls over its computer environment;
- Reviewed DoITT Citywide Technology Policies and Guidelines including: *Citywide Information Security Policy*, *Data Classification Policy, Identity Management Security Policy, Identity Management Standards, User Responsibilities Policy, Password Policy, Chief Information Security Officer Policy, Vulnerability Management Policy, Vulnerability Management Standards, and Application Security Policy* to determine whether DDC had adequate IT controls;
- Interviewed various DDC officials from the Infrastructure Division, Office of Equal Employment Opportunity, Office of Diversity and Industry Relations, and Payroll to better understand their daily tasks and operations;
- Conducted business and system walk-throughs with DDC officials to understand the agency's business operations and the systems used by the responsible units; and
- Reviewed DDC's Password Policy to understand agency's practice on password controls.

To determine whether DDC has adequate system security, we:

- Requested and reviewed DDC's network diagram to determine the presence of adequate security controls that safeguard DDC systems and data;
- Conducted a data center walkthrough to ensure DDC has adequate physical security to protect its computer environment;
- Reviewed DDC's data center relocation project plan to understand the scope and deliverables;
- Analyzed DDC's internal reports including DDC's threat detection reports, incident reports, McAfee reports, and IBM AppScan to determine whether DDC is actively monitoring its systems;

- Analyzed the Vulnerability Remediation Report and Top Remediation Reports from February 2019 to May 2019 to determine whether DDC has actively monitored and addressed the security risks in a timely manner; and
- Reviewed DDC's backup policies, disaster recovery plan, and business contingency plan to ensure DDC has the adequate policies to recover data and continue operations within a reasonable time after disastrous events.

To determine whether DDC has adequate access control, we:

- Reviewed account provisioning and disabling documentation to determine whether DDC has policies and procedures in place for creating the accounts of new users and terminating the accounts of inactive users;
- Reviewed the DDC Password Policy to determine whether the policy complies with DoITT's *Identity Management Standard*, *Identity Management Security Policy*, and *Password Policy*;
- Analyzed and reviewed the agency application listing provided by DDC in September 2018 totaling 43 applications to understand the assess and security controls set up for those applications;
- Conducted access control walkthroughs and tests for all 19 critical systems to determine whether DDC enforces the timeout, lockout features, and proper accesses for each system user as required by DDC and DoITT policies;
- Conducted password control tests such as password format, length and complexity for four of DDC's critical systems that require password login to determine whether DDC's password setups meet the requirements of applicable DDC and DoITT policies;
- Obtained and analyzed the active network user list (as of December 24, 2018) to determine whether users who had not logged on to the network for over 60 days were promptly disabled;
- Compared the list of DDC's active network users with the City's PMS records to test whether users who no longer work for DDC may still inappropriately have access to the network and whether these users' access is removed in a timely manner;
- Obtained and analyzed the user lists of DDC critical applications to determine whether DDC appropriately disabled the inactive users' accounts from its computer environment; and
- Obtained and analyzed user provisioning email access requests to determine whether DDC promptly created new user accounts on its computer network.

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 DDC's access controls over its computer systems.

NYC DDC Department of Design and Construction

Lorraine Grillo
Commissioner

December 5, 2019

Ms. Marjorie Landa
Deputy Comptroller for Audit
Office of the NYC Comptroller
1 Centre St. Room 1100 North
NY, NY 10007

Re: Audit Report on the New York City Department of Design and Construction's Access Control over Its Computer Systems – SI19-058A

Dear Deputy Commissioner Landa,

DDC appreciates the opportunity to review and respond to the *Audit Report on the New York City Department of Design and Construction's Access Control over Its Computer Systems*.

In July of 2018 when I was appointed Commissioner of DDC, I undertook an agency-wide review of its business practices, which resulted in DDC's Strategic Blueprint for Construction Excellence. In issuing this roadmap, the agency renewed its focus on the bottom line – the timely delivery of great projects for the people of New York. As everyone has recognized, DDC has successfully delivered some of the largest and most important public work projects in New York City. As a reflection of its success, DDC's portfolio continues to grow, with a record amount of construction in progress and several large programs affecting millions of New Yorkers in the works.

A key element of DDC's strategic plan is a recognition that the time has come to modernize DDC's internal systems and technology. The plan is to implement a suite of improvements that will transform basic operations and use data to improve business practices. The strategic plan outlined three key components: (i) implement a comprehensive information technology strategy; (ii) create and use standard operating procedures; and (iii) develop complex program management teams.

In implementing a comprehensive information technology ("IT") strategy, DDC will upgrade legacy project management systems to modern standards and create collaborative tools to empower and link all individuals playing a role in a project. This is an exciting time to be evaluating technology as emerging trends such as big data, analytical metrics, 3D modeling, virtual reality, integrated management practices, and wireless – cloud-based communications will continue to advance how construction is performed in the future.

The two-year IT strategic plan will upgrade legacy project management systems to facilitate project work and adapt to business process change over time. The plan will also provide an internet-facing portal for centralized access to agency systems from anywhere. DDC is committed to ensuring that there are adequate controls over computer systems and is pleased the auditors recognized that DDC has established policies, procedures and guidelines for security and access controls to protect information in its computerized environment. As it pertains to the findings concerning certain access and security weaknesses, DDC has been and continues to assess its current IT infrastructure as the agency builds out and upgrades its IT.

In a final note, we are conducting a search for a new Chief Information Officer as our last one received an opportunity with an organization much larger than DDC. The candidate, once selected, will be in charge of completing the current planned upgrade, as well establish a plan of action that allows for growth and change in an industry that constantly changes with updates, while all at the same time mindful of security issues in the IT universe and to protect DDC's project management data.

These are exciting times in IT as cloud-based solutions and hand-held devices are changing how all industries do business. DDC looks forward to cloud-based solutions and new collaboration platforms that allows for increased efficiencies as the agency continues to focus on the bottom line – delivering public work projects for the people of New York City.

In reference to the Audit Report's Recommendations:

Recommendation 1: Promptly update and upgrade all outdated software and hardware that had been identified in its data center review.
Recommendation 2: Develop a plan to timely address the physical and environmental vulnerabilities at the data center until the relocation is completed.
Recommendation 3: Expedite the new data center project to resolve space, power and cooling issues.

Response: It is not clear what is meant by 'promptly' as DDC complies with the City's procurement rules, which have built in time-periods for each step. Nevertheless, DDC is in the process of building and procuring applications to replace legacy applications. All new applications will be hosted in a cloud-based infrastructure, which will help to mitigate space, power, and cooling issues. An updated request for a new data center will be included in IT's FY2021 budget for approval by DoITT and OMB.

Recommendation 4: Perform a periodic risk assessment of all IT assets to evaluate and address all risks associated with its computer environment.

***Response*:** Weekly risk assessments are performed by DoITT and these issues are promptly reviewed and remediated by DDC to reduce the risks of potential threats.

Recommendation 5: Immediately address and resolve all vulnerabilities identified in the 2019 scan reports and obtain a follow-up vulnerability scan report to confirm that the vulnerabilities have been resolved.

Response: Vulnerabilities discovered in the 2019 scan reports that can be addressed have been addressed. Those that have not been addressed were not addressed because doing so would compromise functionality to the legacy applications that DDC is working to replace. Once the applications are replaced, the vulnerabilities will be reduced.

Recommendation 6: Ensure periodic vulnerability scans are conducted, reviewed and promptly resolved to reduce the risks of potential threat.

Response: Vulnerability scans are conducted weekly and potential threats are discussed and remediated or addressed. Resources for which we cannot apply the recommended remedies are continually monitored and backed-up to reduce the risk of data loss or functional degradation.

Recommendation 7: Continue to update the COOP and *Disaster Recovery Plan* to reflect changes in the agency business operations and computer environment.
Recommendation 8: Periodically conduct tests of the COOP and disaster recovery plans to ensure the agencies operational ability in the event of a disaster, emergency or system failure.

Response: DDC does this already and will continue to update the COOP and Disaster Recovery Plan as necessary and periodic tests will be conducted as outlined in the plans.

Recommendation 9: Ensure that all inactive network user accounts are immediately disabled and periodically review user account activity to ensure that only active users and providers have access.

Response: All accounts, which includes employees, consultants and interns are being disabled through multiple sources. A nightly script will automatically disable users that HR changes to inactive status. Separation reports are sent when a user's effective end date is entered into the Active Directory ("AD") to cease the account. Additionally, accounts are automatically ceased after 90 days of inactivity per DoITT's policy.

Recommendation 10: Enforce the policy of disabling user accounts that have not been used to log into the system in over 60 days.
Recommendation 11: Immediately disable – in its network and critical applications- the user accounts of former employees and employees on long-term leave.

Response: DDC makes every effort to ensure that only its active employees retain access to its computer systems. In accordance with DoITT's policy for City agencies, DDC currently has a 90-day policy for disabling user accounts that have not been logged into.

Recommendation 12: Review and assess all [redacted] user accounts to ensure each user is currently authorized and needs access.

Response: [redacted] does not contain sensitive information and all active AD users are authorized to have access to view the information contained within [redacted].

Recommendation 13: Immediately investigate the instances of users with the wrong ERNs, including the assignment of what should be unique ERNs to multiple users, to reduce the risk of granting access to users who are not authorized to have it.
Recommendation 14: Review all user accounts to ensure the information associated with each user is accurate and current.
Recommendation 15: Ensure that accounts are created only for authorized users and that all account creations are properly documented.

***Response*:** DDC will continue to monitor for and investigate instances of users with incorrect ERNs and review user accounts to ensure they are authorized, and that information associated with the account is accurate and current. ERNs are not assigned by DDC and errors with numbers are generally due to a scripting issue at DoITT. DDC provides ticket numbers for these instances so that DoITT will work to resolve issues resulting from their script.

Recommendation 16: Promptly upgrade the [redacted] system to ensure its ability and consistent use to send proper, accurate notifications of all relevant personnel actions to time create and disable user accounts in accordance with applicable City policies.

***Response*:** DDC's [redacted] system does not adequately meet the functionality requirements of sending notifications to IT. As a result, DDC's HR personnel has implemented a separation personnel procedure which promptly provides e-mail notifications of all relevant personnel actions to DDC's IT to ensure the timely creation and disabling of user accounts. DDC's IT has an assigned manager who is responsible for ensuring that user accounts are created and disabled in accordance with the applicable City policies.

Recommendation 17: Implement password rules for [redacted] to comply with DoITT's Password Policy to prevent and minimize the risk of unauthorized access.

***Response*:** Passwords entered into [redacted], which is in the process of being phased out, are secondary and not subject to the policy because a user must be logged into AD in order to gain access. Active Directory password requirements comply with the complexity standard of DoITT's Password Policy to prevent unauthorized access.

As indicated above and in conclusion, DDC is committed to ensuring there are adequate controls over our computer systems. DDC wishes to thank the Comptroller's office and appreciates the time and effort devoted by its audit staff in completing this Report.

Sincerely,

Lorraine Grillo

Lorraine Grillo
Commissioner