# 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 Environmental Protection's Access Controls over Its Computer Systems at the Bureau of Water and Sewer Operations

SI19-061A
**June 26, 2019**
**https://comptroller.nyc.gov**

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

June 26, 2019

To the Residents of the City of New York:

My office has audited the New York City Department of Environmental Protection's (DEP's) Bureau of Water and Sewer Operations (BWSO) to determine whether it has adequate system security and access controls in place to protect the information in its computer environment. We perform audits of this type of the information technology systems maintained by City agencies such as DEP 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 that DEP has established policies, procedures, and guidelines for access controls and security controls to protect information in its computerized environment. However, we found weaknesses in certain of those access and security controls. Specifically, user access had not been disabled for inactive users and former City employees, which could increase security risks. In addition, DEP did not develop and implement a formal agency-wide business continuity and disaster recovery plan to prevent the loss of critical information and operational ability in the event of a disaster or system failure. Finally, DEP maintained outdated servers that have not been supported by the manufacturer since 2015.

The audit makes 16 recommendations including that DEP should ensure that all user accounts assigned to former employees and employees on long-term leave are immediately 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 business continuity plan and disaster recovery plan for all mission-critical applications.

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

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

# TABLE OF CONTENTS

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

## Audit Report on the New York City Department of Environmental Protection's Access Controls over Its Computer Systems at the Bureau of Water and Sewer Operations

## SI19-061A

# EXECUTIVE SUMMARY

This audit was conducted to determine whether the New York City (City) Department of Environmental Protection's (DEP's) Bureau of Water and Sewer Operations (BWSO) had adequate system security and access controls in place to protect the information in its computer environment. DEP's BWSO provides the City with reliable, environmentally sustainable, and cost effective distribution of clean water, collection of wastewater, and management of storm water while assuring the integrity of the sewer infrastructure.

To accomplish its business operations, BWSO uses five mission-critical applications which may contain public, sensitive, private, and confidential information. DEP is responsible for ensuring that it has policies and procedures in place to protect its IT assets and the information stored within its computerized environment.

## Audit Findings and Conclusions

The audit found that DEP has established policies, procedures, and guidelines for access controls and security controls to protect information in its computerized environment. However, we found weaknesses in certain of those access and security controls. Specifically, user access had not been disabled for inactive users and former City employees, which could increase security risks. Also, for two BWSO mission-critical applications, DEP did not implement and enforce the Department of Information Technology and Telecommunications' (DoITT's) password expiration and complexity rules, which are intended to allow only authorized users to gain access to City applications and systems.

In addition, DEP did not perform intrusion detection and vulnerability scans to identify security weaknesses and threats to the servers located in its data center. Furthermore, DEP did not develop and implement a formal agency-wide business continuity and disaster recovery plan to prevent the loss of critical information and operational ability in the event of a disaster or system

failure. Finally, DEP maintained outdated servers that have not been supported by the manufacturer since 2015.

## Audit Recommendations

To address the issues, we made 16 recommendations to DEP, including the following:

- Reassess its current user accounts to ensure that users are given access only to those applications which are authorized and necessary for them to perform their job duties.
- Immediately disable user accounts of former and inactive employees in all of its network and applications.
- Reassess and revise its current policy to ensure that users are positively authenticated and authorized to access its network and applications.
- Reassess all generic accounts in or connected to its computer environment and replace them with unique user accounts for which each individual user is identified and accountable.
- Enforce and update user accounts to include all essential fields required by DEP's User Account Creation procedure.
- Enforce the 15 minutes inactivity logoff rules for all BWSO's mission-critical applications.
- Periodically perform system intrusion and vulnerability scans to ensure that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.
- Perform a periodic risk assessments of all mission-critical applications.
- Develop a formal business continuity plan and disaster recovery plan for all mission-critical applications.
- Enforce the DEP's *Internet Usage Policy* to ensure that all unauthorized software downloads are denied.

## Agency Response

In its response, DEP stated, "[w]e have reviewed the Report and agree with many of the findings and recommendations." DEP also stated that it "will work to implement any appropriate recommendations contained in the final report." However, DEP did not specifically address certain recommendations by stating whether it agreed or disagreed with them, and the agency stated that it had concerns with several audit findings and associated recommendations, including those relating to the lack of vulnerability scans and the continued existence of active user accounts of former and on-long-term-leave employees involving the agency's network and one or more applications. As stated in the report, DEP did not provide documentation to support its assertions concerning these findings and recommendations, and therefore we find no basis to change them. The full text of DEP's response is included as an addendum to this report.

# AUDIT REPORT

## Background

DEP manages the City's water supply, which provides more than one billion gallons of high quality drinking water daily to more than eight million New York City residents, and maintains the City's water distribution network and sanitary sewage collection systems. DEP's BWSO provides the City with reliable, environmentally sustainable, and cost effective distribution of clean water, collection of wastewater, and management of storm water while assuring the integrity of the sewer infrastructure.

BWSO's mission-critical applications and their uses include:

- Computerized Maintenance Management System (CMMS) to streamline workflows including for change management, and to track inventory and manage assets;
- Geographical Information System (GIS) for geographical mapping, querying, and modeling DEP-specific assets including water distribution systems and sewer collection systems;
- Infor Public Sector (IPS) system to manage assets, inventory, repairs, maintenance, and inspections of DEP's environmental infrastructure;
- Water and Sewer Permit System (WSPS) for professionals to apply for City water and sewer work permits; and
- Wonderware to deliver real-time data relating to administration of water and sewer flow.

BWSO uses these five mission-critical applications to accomplish its business operations. These applications may contain public, sensitive, private, and confidential information, such as the locations of existing and future water distribution systems and sewer collection systems.

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. DEP 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 DEP's BWSO had adequate system security and access controls in place to protect the 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 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 August 2018 through May 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 DEP officials during and at the conclusion of this audit. A preliminary draft report was sent to DEP and was discussed at an exit conference held on May 30, 2019. The discussions with DEP officials and its submission of additional information were considered in preparation of the draft report. On June 5, 2019, we submitted a draft report to DEP officials with a request for written comments. We received a written response from DEP officials on June 19, 2019. In its response, DEP did not address several specific audit recommendations made in the audit report. However, DEP stated, "[w]e have reviewed the Report and agree with many of the findings and recommendations." The agency also stated that "DEP will work to implement any appropriate recommendations contained in the final report."

In addition, DEP stated that it was concerned with several of the audit findings and recommendations, including those related to the lack of intrusion detection and vulnerability scans and the continued access of former and on-leave employees to DEP's computer environment. With regard to the intrusion detection and vulnerability scans, the agency stated that "DEP did perform these functions periodically prior to the audit and commenced doing so on a regular basis near the start of the audit." Our audit did not find evidence, and DEP has not provided evidence with its response, to support the assertion that DEP conducted these scans before the audit or that it acted to ensure that any vulnerabilities discovered through such scans were reviewed and remediated. DEP also stated that "DEP does indeed '… ensure that users are positively identified and authorized to access its network and applications.'" As stated in the audit report, we found that 607 users of DEP's network were listed in the City's payroll system as former employees or employees on long-term leave. After carefully reviewing DEP's response, we find no basis to change any of the report's findings or recommendations.

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

# FINDINGS AND RECOMMENDATIONS

The audit found that DEP has established policies, procedures, and guidelines for access controls and security controls to protect information in its computerized environment. However, we found weaknesses in certain of those access and security controls. Specifically, user access had not been disabled for inactive users and former City employees, which could increase security risks. Also, for two BWSO mission-critical applications, DEP did not implement and enforce DoITT's password expiration and complexity rules, which are intended to allow only authorized users to gain access to City applications and systems.

In addition, DEP did not perform intrusion detection and vulnerability scans to identify security weaknesses and threats to the servers located in its data center. Furthermore, DEP did not develop and implement a formal agency-wide business continuity and disaster recovery plan to prevent the loss of critical information and operational ability in the event of a disaster or system failure. Finally, DEP maintained outdated servers that have not been supported by the manufacturer since 2015.

## Access Control Weaknesses

DoITT's *Identity Management Security Policy* states, "[u]ser accounts will be created and de-provisioned in a timely manner." In accordance with that Citywide policy, DEP 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, inactive user accounts were not disabled and former and on-leave employees still had access to the network and mission-critical applications. In addition, DEP utilized generic accounts and did not enforce password controls in two of BWSO's mission-critical applications.

### Inactive User Accounts Were Not Disabled

DEP has adopted policies and 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 9,104 network user accounts DEP listed as active in January 2019 and found that 649 (7 percent) of those user accounts had been inactive for more than 90 days. Our tests also found an additional 861 (9.5 percent) user accounts that had not been logged into since the accounts were initially created, anywhere from over 90 days to 13 years earlier. Without adequate access controls and continuous monitoring, including promptly identifying and disabling inactive accounts, DEP 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 BWSO's mission-critical applications and found that on one application, 203 (29 percent) of 692 user accounts had been inactive for over 90 days. We also found that an additional 173 (25 percent) of the 692 user accounts were listed as active even though the users had *never* logged into the application anywhere from over 90 days to 11 years prior.

Without properly validating and updating access permissions in accordance with the user's actual functional work requirements, which can change over time, and disabling inactive users promptly, DEP is at risk of someone's gaining unauthorized access to its network, which potentially could lead to exposure, theft, modification, or deletion of sensitive information. We forwarded our lists

of inactive users to DEP officials, and they stated that they would review and address the above-mentioned deficiencies.

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

Timely deactivation of user accounts is necessary for the security of sensitive and private data that exists in DEP's computer environment. In that regard, *DoITT's Identity Management Security Policy* states, "[u]ser accounts will be created and de-provisioned in a timely manner." However, when we analyzed the list of current network users and compared it with the City's Payroll Management System (PMS) database, we found that 607 network users were listed in PMS as former employees or employees on long-term leave. We found that 147 (24 percent) of those 607 users had logged into the network after they left DEP or began long-term leave.

In addition, DEP provided a list of user accounts with remote access to its network. Remote access allows a user to access DEP's network from a remote location, for instance from the user's home. We found that 31 (4 percent) of 871 active remote-access users were no longer working for DEP but still had access to its network. We provided a list of the 31 remote-access users to DEP officials and they stated that many of them were currently-active employees but did not provide any documentation to support that assertion.

We also analyzed the BWSO's mission-critical applications' user accounts to determine whether they were assigned to active and authorized employees. We found that 16 users on one application and 11 users on another application were listed as retired, terminated, or on leave in PMS, but still had access to DEP's network and the two applications. The continued existence of active user accounts assigned to individuals who no longer work for DEP—and therefore presumably are not authorized users of its information systems—creates a vulnerability that could be exploited to compromise the integrity, confidentiality, and availability of the agency's critical applications and the data therein. Without continual monitoring of its users' access, DEP may increase the risks of security breaches and the opportunity for the applications' misuse.

Moreover, DEP policy is to forward the list of departed users to its Bureau of Business Information Technology (BBIT) for the purpose of deactivating their user access. On January 14, 2019, we analyzed a list of employees who left the agency from July 2018 through September 2018 and compared the users to the network user list to ensure their accesses were disabled. We found that four users and one administrator still had access to the agency's network. Adequate access controls and continual monitoring—including to identify and eliminate inactive accounts as above mentioned—are necessary to minimize DEP information systems' vulnerability to security breaches and the opportunity for misuse agency resources. We forwarded the issues to DEP officials, and they responded that they will review and disable the inactive accounts.

## Utilization of Generic User Accounts

DoITT's *Identity Management Security Policy* states, in part, "4) Users must be positively and individually identified and validated prior to being permitted access to any City computing resource. 5) Users will be authenticated at a level commensurate to the data classification of the information being accessed. 6) Access permissions must be defined in accordance with a user's actual functional work requirements." However, we found that over 200 generic user accounts that were not assigned to specific, individual users existed in DEP's computer environment. In response to our inquiries, DEP responded that the generic accounts were created for conference room and training purposes.

A generic account may be shared by multiple users, making it difficult to identify or track the specific individual(s) who have access to the network at any given time. These users could potentially make unauthorized changes to the data or sensitive information stored in or transmitted through the agency's computer system. These generic accounts create a lack of accountability and a gap in the audit trail and jeopardize the computer environment. Without security controls over generic accounts, or the ability to identify the individuals with access, the agency incurs an increased risk of unauthorized access and exposure of sensitive information.

## Inadequate User Account Profiles

DEP's *User Account Creation* procedure specifies that all network accounts must contain the information that the required fields call for, including the users' first name, last name, department, and employee type. However, we found that 2,883 (32 percent) of 9,104 network user accounts were missing one or more items of the required information. We also found that DEP erroneously created duplicate network user accounts for 23 employees. We discussed this issue with DEP officials, and they agreed to remove the duplicate accounts. Without accurately creating and maintaining user account information, DEP minimizes its ability to identify, detect, and govern user accounts within its network.

## Inadequate Password Controls over Administrative and Service Accounts

DoITT's *Password Policy* states that administrative accounts *should* be, and service accounts *must* be, restricted to logging in from specified Internet Protocol (IP) addresses. The policy also requires additional security protocols for non-expiring service-account passwords, specifically, that they have a minimum length of 15 characters and be either randomly generated or highly complex.

We found that the non-expiring administrative accounts and service accounts were not restricted to logging in from specified IP addresses and did not meet the DoITT's password-length and complexity requirements. These accounts are allowed to create, edit, delete, and modify information within DEP computer environment. Without enforcing the required password controls, DEP incurs an increased risk of unauthorized access and exposure of sensitive information. We discussed the issues with DEP officials, and they informed us that they are in the process of implementing a solution to comply with DoITT's *Password Policy*.

## Two Mission-Critical Applications Did Not Comply with DoITT's *Password Policy*

We found that two mission-critical applications, which contain sensitive data, did not comply with the DoITT's *Password Policy*, which requires that passwords:

- 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.
- Must expire at least every ninety (90) days, with the exception of some parameters in Administrative and Service accounts.
- Must have a minimum length of eight (8) characters.
- Must not be reused for four (4) iterations.

- Must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character.

Without compliance with the DoITT's *Password Policy*, unauthorized users could potentially guess the password and thus might gain access to these critical applications and the information they contain.

At the exit conference, DEP officials stated that they will revise the password parameters to comply with DoITT's *Password Policy*.

## Failure to Implement DEP's Inactivity Logoff Requirement for BWSO's Mission-Critical Applications

DEP's *Login Policy* states, "[t]he scope of the policy includes all logins to critical applications and servers, irrespective of their operating platforms . . . [t]he system should log-off automatically after inactivity of fifteen minutes or a period specified by the Information Security Officer." However, our tests found that none of BWSO's five mission-critical applications complied with the above-mentioned policy requirement to log-off users after 15 minutes of inactivity. For instance, after 20 minutes of inactivity, we were logged-off from an application and we were required to log-in to the system by entering the user ID and password to re-authenticate. We also found that two applications did not implement the inactivity logoff requirement at all. These two applications contain confidential data, such as water sensor locations. DEP officials stated that they did not implement the 15 minutes-logoff feature to their mission-critical applications. DEP issued these standards as a measure of protecting the information, but without enforcement, DEP is exposed to an increased risk of unauthorized access and exposure of sensitive and confidential information.

At the exit conference, DEP officials informed us that they will implement the 15 minutes logoff feature for three mission-critical applications. DEP officials also stated that they will reassess the *Login Policy* for the remaining two applications.

## Recommendations

DEP should:

1. Reassess its current user accounts to ensure that users are given access only to those applications which are authorized and necessary for them to perform their job duties.

   ***DEP Response:*** DEP did not address this recommendation.

2. Immediately disable user accounts of former and inactive employees in all of its network and applications.

3. Immediately disable remote user accounts of former and inactive employees in its network and thereafter conduct periodic reviews to identify and disable the remote user accounts of former and inactive employees.

   ***DEP Response:*** DEP responded to recommendations 2 and 3 by stating, "DEP does disable the user accounts of former employees but sometimes needs to reactivate these accounts at the request of the NYC Department of Investigation, the NYC Law Department, or DEP management. Once the information sought has been retrieved by the requesting entity, DEP again disables these accounts.

These former employees do not have access to DEP's computer environment during these periods of reactivation."

"Inactive user accounts are indeed disabled and the user can only access the account once it has been reactivated by the Bureau of Business Information Technology's (BIT) Service Desk. This does not represent a security risk."

***Auditor Comment:*** As stated in the audit report, DEP did not disable the access of 607 former or on-long-term-leave employees, including 147 users who had logged into the network after they left DEP employment or began long-term leave. DEP provides no support for its argument that these accounts may have been reactivated at the request of DEP management or another agency, or that the "former employees do not have access to DEP's computer environment during these periods of reactivation." Therefore, we strongly recommend that DEP review and disable these user accounts.

4. Reassess and revise its current policy to ensure that users are positively authenticated and authorized to access its network and applications.

   ***DEP Response:*** DEP stated that "[t]he basis for recommendation 4 is unclear. DEP does indeed '. . . ensure that users are positively identified and authorized to access its network and applications.'"

   ***Auditor Comment:*** As stated in the audit report, DEP did not identify and disable the access of 607 network users and 31 remote-access users who were no longer working for DEP or were on long-term leave but still had access to its network. We therefore urge DEP to reassess its processes and revise its policy and procedures as needed to ensure going forward, and on a continuing basis, that *all* users of its network and applications are positively authenticated and authorized based on their then-current roles and job responsibilities in the agency.

5. Reassess all generic accounts in or connected to its computer environment and replace them with unique user accounts for which each individual user is identified and accountable.

   ***DEP Response:*** "DEP management finds that the use of limited access accounts attached to conference rooms and other shared resources represent very little risk and provide an efficient means of allocating the use of these resources."

   ***Auditor Comment:*** These generic accounts create a lack of accountability and a gap in the audit trail and jeopardize the computer environment. Without adherence to City standards, DEP incurs an increased security risk of unauthorized access and exposure of sensitive information. Therefore, we urge DEP to implement our recommendation.

6. Enforce and update user accounts to include all essential fields required by DEP's *User Account Creation* procedure.

   ***DEP Response:*** DEP did not address this recommendation.

7. Ensure that all administrator and service accounts comply with DoITT's *Password Policy.*

   ***DEP Response:*** DEP did not address this recommendation.

8. Implement password rules for the two mission-critical applications to comply with DoITT's *Password Policy* to prevent and minimize the risk of unauthorized access.

***DEP Response:*** DEP did not address this recommendation.

9. Enforce the 15 minutes inactivity logoff rules for all BWSO's mission-critical applications.

   ***DEP Response:*** "DEP will adjust the inactivity logoff rules for most of its applications but will adjust the policy to account for specific applications that, due to business needs, require longer or no automatic logoff."

# System Security Weaknesses

Information security involves an ongoing process of finding and addressing security gaps, such as by periodically performing vulnerability scans and actively monitoring the security posture of the computer environment. However, our audit found that DEP uses outdated software, did not perform vulnerability scans, and lacks a business continuity and disaster recovery plan.

## Outdated Software

DoITT's *Vulnerability Management Policy* states, in part, "[a]ll City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." Currently, DEP manages its own data centers, which includes hosting several mission-critical applications for BWSO. However, we found that DEP uses outdated software, which has not been supported by the manufacturer since 2015. DEP officials stated that they are planning to upgrade the outdated software, but did not provide the timeline for completion. The agency's failure to ensure that the server operating system software is up-to-date and supported by the manufacturer with security updates and patches may allow attackers to gain access to restricted information and to modify, delete, and steal data.

## Lack of Vulnerability Scans

DoITT's *Vulnerability Management Policy* also states that "[v]ulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation." However, DEP did not conduct periodic system intrusion detection and vulnerability scans to identify and analyze the security weakness within its network and applications. DEP officials stated that they did not perform periodic scans and began conducting vulnerability scans in September 2018, after the start of our audit. A vulnerability scan can help analyze, identify, and classify security weakness and threats to an organization's network and applications. Without promptly remediating the vulnerabilities, DEP may be at risk of security breaches from internal and external sources.

In addition, we performed an assessment of the BWSO's public-facing website and found security vulnerabilities regarding encryption standards that have been publicly disclosed since December 2017. We discussed the issues with DEP officials, who stated that they are aware of these security vulnerabilities and will remediate these issues with DoITT.

## Lack of IT Risk Assessments on All Mission-Critical Applications

Identifying and assessing information security risks are essential to determining what controls are required to protect the information within the computer systems. DEP's *Agency Security Policy* states that "[a] proper Business Impact Analysis and Risk Assessment should be performed for

all critical business systems, either by the Information Security Officer or by an outsourced resource." However, DEP officials stated that they hired a third-party vendor to conduct a partial risk assessment in 2017. The scope of this risk assessment did not include all mission-critical applications. Without an effective risk assessment to evaluate and address all potential risks and threats associated with its computer environment, DEP may be at risk of cyber vulnerabilities and negatively impact the agency operations.

## Lack of Business Continuity and Disaster Recovery Plan

According to DoITT's *Citywide Application Security Policy,* "[a]pplication 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."

DEP is responsible for backup and disaster recovery for all hardware and software hosted in its own data center. However, DEP did not have a formal business continuity plan and disaster recovery plan. A comprehensive business continuity and disaster recovery plan should specify the steps that need to be taken to quickly resume agency operations without material loss of computer data. These plans should include the essential information to determine the operational downtime, resources availability, and recovery procedures. DEP officials stated that they are planning to develop and complete these plans by December 2019.

Without a business continuity plan and a disaster recovery plan, DEP is vulnerable to the loss of mission-critical information and operational ability in the event of a disaster, emergency, or system failure.

## Lack of Enforcement of Internet Usage Policy

DEP's *Internet Usage Policy* states, "[t]he scope of the policy includes all employees, irrespective of their position . . . In case of the downloading of a file having a size more than 10 MB, prior permission from the respective manager is required." The policy further states, "[n]o one is allowed to use the chat services." However, we found that DEP did not enforce its *Internet Usage Policy*. Specifically, on testing one of DEP's computer workstations, we were able to successfully download a social media live chat from the Internet without prior approval or a warning message. By allowing software installation without proper permission, DEP incurs an increased risk of security vulnerabilities and of the unauthorized release of confidential agency data.

## Recommendations

DEP should:

10. Promptly upgrade and update all outdated software that had been identified in above section.

    ***DEP Response:*** DEP did not address this recommendation.

11. Periodically perform system intrusion and vulnerability scans to ensure that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.

***DEP Response:*** "As discussed during the audit and at the exit conference, DEP did perform these functions periodically prior to the audit and commenced doing so on a regular basis near the start of the audit."

***Auditor Comment:*** DEP did not provide documentation to support its current statement that it periodically performed system intrusion and vulnerability scans prior to the audit. As stated in the audit report, DEP began conducting vulnerability scans after the start of our audit. Therefore, we continue to recommend that DEP implement this recommendation, including by conducting the scans periodically and by ensuring that any vulnerabilities discovered are reviewed and remediated to reduce the risks of potential threats.

12. Promptly address and remediate the vulnerabilities within the specified application with DoITT.

    ***DEP Response:*** DEP did not address this recommendation.

13. Perform a periodic risk assessments of all mission-critical applications.

    ***DEP Response:*** DEP did not address this recommendation.

14. Develop a formal business continuity plan and disaster recovery plan for all mission-critical applications.

    ***DEP Response:*** DEP did not address this recommendation.

15. Periodically conduct disaster recovery tests to ensure its operational ability in the event of a disaster, emergency or system failure.

    ***DEP Response:*** DEP did not address this recommendation.

16. Enforce the *Internet Usage Policy* to ensure that all unauthorized software downloads are denied.

    ***DEP Response:*** "It should be noted that the auditors' ability to download and install software on a DEP workstation (recommendation 16) was due to the elevated rights that the auditors were provided with in order for them to access a particular applications."

    ***Auditor Comment:*** DEP asserts that our finding that DEP did not enforce its policy of restricting downloads and prohibiting the use of chat services was based on the elevated rights our auditors received. However, under DEP's *Internet Usage Policy*, no one is allowed to use chat services; no exception is provided for auditors or anyone else. Accordingly, we are concerned that DEP's controls are inadequate to prevent its policy from being circumvented by the granting of elevated rights to users on an *ad hoc* basis.

# 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 August 2018 through May 2019. We conducted the audit fieldwork from December 2018 through May 2019. To achieve the audit objectives, we:

- Reviewed DEP's organizational charts including the agency overall, BBIT and BWSO's to understand its administration and personnel structure;
- Reviewed DEP's Fiscal Year 2019 Mayor's Management Report and DEP's *2018 Strategic Plan* to determine the agency's current goals, objectives, and priorities;
- Conducted system walk-throughs with DEP officials to understand the responsibilities of various BWSO and the functionalities of BWSO's mission-critical applications;
- Reviewed New York City Comptroller's Directive #1 Calendar Year 2017 Checklist to determine whether DEP has proper internal controls;
- Requested DEP's network diagram to determine whether the agency documented its network structure to assess its overall security awareness;
- Reviewed DEP's *Information Security Policy Manual* to determine whether DEP's policies adhere to DoITT policies and guidelines;
- Conducted a walkthrough of DEP's data center to ensure it has adequate physical security to protect its computer environment;
- Requested and reviewed DEP's *Patch Management Policy* to determine whether the agency's has controls in place to support continued system operations;
- Reviewed DEP's OIT *Management and Operations Manual* to determine whether DEP complies with DoITT's *Backup Policy* and *Vulnerability Management Policy*;
- Reviewed documentation to determine whether DEP had policies and procedures in place for creating new users and terminating the accounts of inactive users;
- Reviewed DEP officials provided a risk assessment report conducted by a third-party vendor in June 2017;
- Reviewed DEP's *Login Policy* to determine whether DEP policies complied with DoITT's *Identity Management Standard*, *Identity Management Security Policy*, and *Password Policy*;
- Reviewed DEP's remote user list to determine whether DEP adequately removed access to users that were no longer working or on long term leave as per *DoITT's Remote Access Policy*;
- Conducted password control tests on BWSO mission-critical applications such as password format, length, and complexity as required by DoITTs *Password Policy*;

- Performed access controls tests on mission-critical applications to determine whether DEP enforces the timeout and logout features as required by DEP's *Login Policy*;
- Compared DEP network users list as of January 2019 to PMS to test whether users who were no longer working for DEP were disabled in a timely manner as required by DoITT's *Identity Management Security Policy;*
- Reviewed the departed user lists of DEP network users from July 2018 to September 2018 to determine if DEP appropriately removed the access for these employees that were no longer with DEP as required by DoITT's *Identity Management Security Policy*; and
- Reviewed user lists of BWSO's mission-critical applications to determine whether DEP had adequate user access controls.

The results of the above tests, while not projectable to their respective populations, provided a reasonable basis for us to evaluate and support our findings and conclusion about DEP's access controls over its computer systems.

NYC Environmental Protection

*Vincent Sapienza, P.E.*
*Commissioner*

**Joseph P. Murin**
Chief Financial Officer
JMurin@dep.nyc.gov

59-17 Junction Boulevard
Flushing, NY 11373
T: (718) 595-6936
F: (718) 595-3525



June 19, 2019
Ms. Marjorie Landa
Deputy Comptroller for Audit
Office of the Comptroller
1 Centre Street, Room 1100
New York, NY 10007

Re: Audit Report on the Department of Environmental Protection's Access Controls over Its Computer Systems at the Bureau of Water and Sewer Operations

Dear Ms. Landa:

Thank you for the opportunity to comment on the New York City Comptroller's draft report on the Department of Environmental Protection's (DEP) Access Controls over Its Computer Systems at the Bureau of Water and Sewer Operations (the Report). We have reviewed the Report and agree with many of the findings and recommendations.

We are concerned, however, with several of the findings and the recommendations associated with those findings.

- The draft report indicates that "…DEP did not perform intrusion detection and vulnerability scans…" As discussed during the audit and at the exit conference, DEP did perform these functions periodically prior to the audit and commenced doing so on a regular basis near the start of the audit.
- As discussed prior to and at the exit conference, DEP does disable the user accounts of former employees but sometimes needs to reactivate these accounts at the request of the NYC Department of Investigation, the NYC Law Department, or DEP management. Once the information sought has been retrieved by the requesting entity, DEP again disables these accounts. These former employees do not have access to DEP's computer environment during these periods of reactivation.
- Inactive user accounts are indeed disabled and the user can only access the account once it has been reactivated by the Bureau of Business Information Technology's (BIT) Service Desk. This does not represent a security risk.
- The basis for recommendation 4 is unclear. DEP does indeed "…ensure that users are positively identified and authorized to access its network and applications."
- Concerning recommendation 5, DEP management finds that the use of limited access accounts attached to conference rooms and other shared resources represent very little risk and provide an efficient means of allocating the use of these resources.

- As discussed previously, DEP will adjust the inactivity logoff rules for most of its applications but will adjust the policy to account for specific applications that, due to business needs, require longer or no automatic logoff. It should be noted that the automatic Windows screen lock still provides security in these instances.
- It should be noted that the auditors' ability to download and install software on a DEP workstation (recommendation 16) was due to the elevated rights that auditors were provided with in order for them to access a particular applications (Avantis).

In addition to the above comments, DEP has a few concerns with some of the wording in the report as discussed below:

1. Concerning the second paragraph of the Executive Summary, it would be better if the sentence read "…which *can* contain public, sensitive, private, and*/or* confidential information."
2. In the Background section, there are two times where sewer connections are mentioned. We believe those references should be to sewer *collection systems*. Also, please see note 1, above for the description of the information contained in these computer systems.

Thank you for your time and attention to our written responses. DEP will work to implement any appropriate recommendations contained in the final report. We are available to respond to and assist with any questions you may have.

Sincerely,

Joseph P. Murin
Chief Financial Officer

Cc: A. Georgelis
C. McMaster
M. Ritze