# 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 Security Controls at the New York City Department of Sanitation over Its Computer Systems

SI18-115A
**April 30, 2019**
**http://comptroller.nyc.gov**

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

April 30, 2019

To the Residents of the City of New York:

My office has audited the New York City Department of Sanitation's (DSNY's) security and access controls over its computer systems to determine whether DSNY had adequate security and access controls in place to protect the information in its computerized environment. We conduct computer system audits such as this to help ensure the security and 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 DSNY has implemented controls for application access and data protection, and has implemented security controls to protect its computerized environment. However, we found weaknesses in certain access and security controls. Specifically, with regard to access controls, DSNY did not properly deactivate or disable the application user accounts of 583 former or on-leave employees. The audit also found weaknesses in application security controls including: use of generic login IDs; use of passwords that do not expire after 90 days; use of passwords that do not comply with password length and complexity rules; use of an application that does not lock out after consecutive failed logons; and the use of an insecure network protocol in web-based applications.

Further, we found that hand-held devices in use had unsupported hardware and software, and store unencrypted information in a removable memory card. In addition, we found that one critical application stores scanned documents without adequate protection. Further, we found that the agency has not conducted vulnerability scans on three critical applications, and the network vulnerability scans it has run produced reports that are unreliable. Lastly, we note that DSNY has fully implemented only two out of seven recommendations from a security assessment it obtained from a third-party vendor in 2016.

The audit makes 12 recommendations, including: that DSNY immediately disable former and inactive employees' user accounts in all of its applications and implement procedures to ensure that going forward frequent periodic reviews are conducted to promptly identify and disable the application user accounts of former and inactive employees; that DSNY remove all generic logins from its application and replace them with unique user logins; that DSNY complete the roll-out of the new hand-held devices and decommission old ones, as planned; and that DSNY ensure all web-based applications utilize the secure HTTPS protocol.

The results of the audit have been discussed with DSNY 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

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 AND SPECIAL REPORTS
# IT AUDIT

## Audit Report on the Security Controls at the New York City Department of Sanitation over Its Computer Systems SI18-115A

# EXECUTIVE SUMMARY

We audited the New York City Department of Sanitation's (DSNY's) security and access controls over its computer systems to determine whether DSNY had adequate critical system security and access controls in place to protect the information in its computerized environment.

DSNY is the world's largest sanitation department, collecting more than 10,500 tons of residential and institutional garbage and 1,760 tons of recyclables every day. DSNY also clears litter, snow, and ice from some 6,500 miles of streets, removes debris from vacant lots, and clears abandoned vehicles from City streets. The Department has a workforce of nearly 10,000 employees and utilizes approximately 6,000 vehicles to fulfill its critical mission.

As part of its operations, DSNY uses 136 computer applications, and has identified 10 of them as critical. This audit examined those 10 critical applications and 10 other randomly selected non-critical applications.[1] DSNY describes critical applications as "applications that are core to the operation of a business, and need to be operating properly whenever the business is operating. Failure or disruption of a critical system will result in serious impact or failure of the business operations."

## Audit Findings and Conclusions

The audit found that DSNY has implemented controls for application access and data protection, and has implemented security controls to protect its computerized environment. However, we found weaknesses in certain access and security controls. Specifically, with regard to access controls, DSNY did not deactivate or disable the application user accounts of 583 former or on-leave employees. The audit also found weaknesses in application security controls including: use of generic login IDs; use of passwords that do not expire after 90 days; use of passwords that do not comply with password length and complexity rules; use of an application that does not lock

[1] The critical and non-critical application names and descriptions were not included in the final version of this report due to the sensitivity of the information and the potential risk associated with the release of such information.

out after consecutive failed logons; and the use of an insecure network protocol in web-based applications.

Further, we found that the hand-held devices use unsupported hardware and software, and store unencrypted information in a removable memory card. In addition, we found that one critical application stores scanned documents without protection. Further, we found that the agency has not conducted vulnerability scans on three critical applications, and the network vulnerability scans it has run produce reports that are unreliable. Lastly, we note that DSNY has fully implemented only two out of seven recommendations from a security assessment it obtained from a third party vendor in 2016.

During the audit and the exit conference on February 8, 2019, DSNY officials informed us of certain steps they are taking to address the issues identified in the audit, which are described in this report.

## Audit Recommendations

To address the abovementioned issues, we make the following 12 recommendations to DSNY:

- Immediately disable former and inactive employees' user accounts in all of its applications and implement procedures to ensure that going forward frequent periodic reviews are conducted to promptly identify and disable the application user accounts of former and inactive employees.
- Remove all generic logins from its application and replace them with unique user logins, each of which identifies and is issued only to an individual employee or other authorized user.
- Update the three applications to comply with DoITT's 90-day password expiration requirement.
- Comply with DoITT's *Password Policy* to ensure that passwords that provide access to its applications meet the prescribed standards for length (minimum-number-of characters) and complexity.
- In accordance with DoITT standards, ensure that user accounts are locked and remain locked for a minimum of 15 minutes after five sequential invalid login attempts.
- Complete the roll-out of the new hand-held devices and decommission old ones, as planned, to address the security risks posed by the use of outdated and unsupported hardware and software from the old hand-held devices in use as of the date of this report.
- Ensure that data encryption and security features are enabled in all new hand-held devices to protect the data they store and transmit.
- Ensure all web-based applications utilize the secure HyperText Transfer Protocol Secure (HTTPS).
- Ensure all scanned documents are protected with encryption.
- Periodically conduct necessary vulnerability scans of critical applications, address any vulnerabilities found, and conduct a follow up scan to confirm vulnerability remediation, as directed in DoITT's *Vulnerability Management Policy*.

- Test all vulnerability scanning tools to assess the reliability of the scanning results, and correlate the results from vulnerability scanning tools with the output of other security tools, as recommended by the National Institute for Standards and Technology (NIST).
- Ensure that the third-party vendor recommendations made in the 2016 security assessment report are implemented.

## Agency Response

In its response, DSNY generally agreed with 7 of the 12 recommendations and partially agreed with 2 recommendations. At the same time, DSNY took issue with some findings in this report. However, DSNY stated, "The audit report identified weakness that need to be addressed to protect the information in DSNY's computerized environment. We will continue working to improve our system security and access controls and to incorporate your recommendations where practical."

The full text of DSNY's response, redacted only to exclude the names of specific systems due to the sensitivity of the information contained in this report, is included as an addendum to this report.

# AUDIT REPORT

## Background

The New York City Department of Sanitation (DSNY) is the world's largest sanitation department, collecting more than 10,500 tons of residential and institutional garbage and 1,760 tons of recyclables every day. DSNY also clears litter, snow, and ice from some 6,500 miles of streets, removes debris from vacant lots, and clears abandoned vehicles from City streets. The Department has a workforce of nearly 10,000 employees and utilizes approximately 6,000 vehicles to fulfill its critical mission.

DSNY's mission is to keep New York City healthy, safe, and clean. As part of its operations, DSNY uses 136 computer applications, and has identified 10 of them as critical. This audit examined those 10 critical applications and 10 other randomly selected non-critical applications. DSNY describes critical applications as "applications that are core to the operation of a business, and need to be operating properly whenever the business is operating. Failure or disruption of a critical system will result in serious impact or failure of the business operations."

The agency's 10 critical and 10 non-critical applications may contain private information in addition to public data. The private information that is collected, processed, transmitted, or stored by these applications includes personal health information, private carting business information, agency personnel information, and information restricted to agency use, such as staff drug test results, staff usernames, and application configuration information. According to the New York City Department of Information Technology and Telecommunications' (DoITT's) *Citywide Information Security Policy*, information stored in an agency's applications must be placed in a secure environment and protected from unauthorized access. To accomplish that level of security, adequate access controls, such as user-authorization, identification, authentication, access-approval, and login credentials are essential. DSNY is also responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment, which includes complying with DoITT's policies and standards.

## Objective

The objective of this audit is to determine whether adequate critical system security and access controls are in place to protect information in the agency's computerized environment.

## Scope and Methodology Statement

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our 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 is March 2018 through November 2018. Please refer to the Detailed Scope and Methodology at the end of this report for the specific procedures and tests that were conducted.

## Discussion of Audit Results

The matters covered in this report were discussed with DSNY officials during and at the conclusion of this audit. A preliminary draft report with all of the systems that were the focus of the audit clearly identified was sent to DSNY and was discussed at an exit conference on February 8, 2019. On March 15, 2019, we submitted a draft report with all of the systems that were the focus of the audit clearly identified to DSNY with a request for comments. We received a written response on March 29, 2019. In its response, DSNY generally agreed with 7 of the 12 recommendations and partially agreed with 2 recommendations. At the same time, DSNY took issue with some findings on this report. However, DSNY stated, "The audit report identified weakness that need to be addressed to protect the information in DSNY's computerized environment. We will continue working to improve our system security and access controls and to incorporate your recommendations where practical."

The full text of DSNY's response, redacted only to exclude the names of specific systems due to the sensitivity of the information contained in this report, is included as an addendum to this report.

# FINDINGS AND RECOMMENDATIONS

The audit found that DSNY has established controls for application access and data protection, and has implemented security controls to protect its computerized environment.[2] However, we found weaknesses in certain access and security controls. Specifically, DSNY did not deactivate or disable the application user accounts of 583 former or on-leave employees as required by DoITT's policies, increasing the risk that unauthorized users could gain access to one of the affected applications and attempt to modify, delete, or steal data. In addition, the following security control weaknesses were identified:

- DSNY allowed multiple individuals to use generic login IDs to access one critical application.
- DSNY did not enforce DoITT's 90-day password-expiration rule for three of its applications, two critical, and one non-critical.
- DSNY did not enforce DoITT's password's minimum-length and/or complexity rules for three of its critical applications.
- DSNY did not lock users' application access after a predetermined number of unsuccessful login attempts for three of its critical applications.
- DSNY uses the unsecured network protocol HyperText Transfer Protocol (HTTP) for four of its web-based applications, two critical and two non-critical.

The audit also found that the hand-held devices are outdated and consequently are affected by security weaknesses, such as the use of unsupported hardware and software, and the storage of unencrypted information in a removable memory card. Moreover, another DSNY critical application stores unencrypted scanned documents. Further, the agency has not conducted vulnerability scans on three critical applications, and according to DSNY, the network vulnerability scans that were conducted are unreliable. Finally, DSNY has fully implemented only two out of seven recommendations from the security assessment it received more than two years ago from a contracted consultant and consequently remains noncompliant or not fully compliant with applicable DoITT policies in areas such as: (1) a data classification program; (2) a Software Development Life Cycle (SDLC) process that identifies and remediates vulnerabilities; (3) a security training and awareness program; and (4) a disaster recovery plan to address the effects of a potential agency-wide disruptive cyber event.

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

[2] In addition to its own controls, DSNY's computer infrastructure is protected by DoITT's security controls, such as antivirus protection, antimalware, and other IT security services.

# Access Control Weaknesses

## Risk of Unauthorized Access to DSNY's Computer Applications through Active User Accounts Assigned to Former or On-leave Employees

DoITT's *Identity Management Security Policy* states, "User accounts will be created and de-provisioned in a timely manner." However, DSNY did not ensure that its user accounts for five critical applications were promptly deactivated for 583 former employees and other inactive users, such as employees on long-term leave.[3]

We compared DSNY's lists of active user accounts for five critical applications as of June 29, 2018 against a list of inactive employees from the City's Payroll Management Systems (PMS) and found that 583 former employees or employees on long-term leave in PMS are listed as active in the multiple user lists provided.[4] DSNY is responsible for creating and monitoring access to its applications for its authorized users and for disabling their access when their employment status changes. Its failure to timely deactivate the user accounts assigned to 583 individuals who either had left agency service or had gone on long-term leave may have exposed its data and that of its clients to the risk of unauthorized access.

Timely deactivation of user accounts assigned to former and on-leave employees is necessary for the security of sensitive data that is stored and accessed through DSNY five applications. The continued existence of active user accounts assigned to individuals who have left DSNY—and therefore are not authorized users of its information systems—creates a vulnerability that could be exploited to compromise the integrity, confidentiality, and availability of the agency's critical applications and the data therein. Accordingly, to protect the City against the risk of unauthorized access to private and confidential information, it is necessary that DSNY promptly deactivate the user accounts of individuals who are no longer authorized to access its applications.

DSNY officials informed us that the agency disabled the accounts after we brought the issue to their attention, stating, "The [application name redacted] accounts that were questionable were investigated/disabled and moved to a departed user OU [organizational unit]. . . . The process going forward is being handled via a new off boarding method that will inform IT of departing users and kick off a process to remove accounts and access."[5]

## One Critical Application Allows the Use of Generic Login IDs

DoITT's *Application Security Policy* states, "All access to City of New York systems must be authorized and based on individual identification and authentication." However, a DSNY application does not comply with DoITT policy in that it has 95 generic login IDs that do not identify a specific individual.[6] During our analysis of active user accounts for critical applications described in the previous section, we found that one application uses generic login IDs. While a

[3] Inactive users may include employees on extended leave, with or without pay, because of factors such as an illness or child care needs, or who are absent from work because of suspension, among other causes. We use the terms deactivated and disabled interchangeably.
[4] The PMS effective date (the date when the individual left DSNY employment or went on extended leave), for the 583 individuals ranges from July 1989 to June 2018.
[5] DSNY's [application name redacted] uses Organizational Units (OUs) to group objects for administrative purposes. The agency stated that it moved the user accounts in question to a specific group container called "departed user OU."
[6] Users log in to the application using generic login IDs that may signify an individual's ostensible role or function, for example, one login for administrators, another for mechanics in a particular location, and a third for other staff members. (For security purposes, the actual generic login IDs provided by DSNY are not repeated here.)

regular user ID identifies and is used by a single employee, a generic login ID can be assigned to multiple employees. For example, a mechanic in a sanitation garage may be assigned a generic login that identifies his or her role and location. The mechanic working the next shift in the same garage will use the same generic login ID.

DSNY explained that there is an operational need for generic login IDs, since the agency assigns and moves personnel quickly, as needed, during periods of heavy demand for staff. To avoid the delay that would result if it had to obtain new credentials when it moves staff who need to access the application, the agency relies on generic login IDs. However, having multiple users using the same generic login ID makes it difficult to identify or track the individuals who make specific changes to the application's data. Thus, generic login IDs create a lack of accountability and a gap in the audit trail which is a critical control over the system. In response to our raising this issue, DSNY officials stated that they plan to switch the current local login/authentication method for the application to a different method—one that leverages the DSNY Active Directory/ Lightweight Directory Access Protocol (LDAP) as an additional level of user-identification and authentication, and thereby endeavor to restore accountability to the continued use of generic login IDs for application access.[7] The agency also stated that the work required to make that change is expected to start mid-April 2019 and end by December 2019.

## Three Applications Did Not Require User Passwords to Expire after 90 Days

DoITT's *Password Policy* states, "User Account passwords and/or PINs must expire at least every 90 days." However, we found that three of DSNY's applications do not comply with DoITT's 90-day password-expiration rule. Having application passwords change periodically lowers the risk that unauthorized users have ample time to guess a password and gain access to the application and its data.

During walkthroughs of 10 critical and 10 non-critical applications, DSNY officials stated that the three abovementioned applications' passwords are not set to expire after 90 days. DSNY informed us that it plans to upgrade one application by June 2019 and that the upgrade should make that application compliant with the 90-day password expiration policy. As for the second application, as mentioned above, DSNY plans to switch from generic logins to Active Directory/LDAP logins, which, if accomplished, would make the application compliant with the password expiration policy. Finally, DSNY officials stated that they have no plan to implement the 90-day password expiration rule in DSNY's third application, since the agency plans to replace it. However, DSNY did not provide a replacement date. Until the three abovementioned applications are made to comply with the 90-day password expiration rule, the applications remain at risk of unauthorized users gaining access to the application and its data.

## Three Critical Applications Did Not Comply with City Requirements for Password Minimum Length and/or Complexity

DoITT's *Password Policy* states that passwords and PINs must have a minimum length of eight characters and must contain at least one alphabetic character and at least one numeric character or special character, such as an exclamation point, a number sign, or a dollar sign among others. Similarly, DSNY's *Password Policy* states that strong passwords contain at least eight characters in length, both upper and lower case characters, and have digits and special/punctuation

[7] LDAP is an Internet protocol for accessing distributed directory services. LDAP is used to create, modify, and delete user account names, track login information, establish access permissions, and enable applications to authenticate users.

characters. However, three of DSNY's critical applications did not comply with one or both requirements—for password-length and complexity—set forth in DoITT's and DSNY's password policies.

During our system test of critical applications, we found that two applications failed to meet the password minimum-length standard required by DoITT's and DSNY's policies.[8] In addition, three applications did not meet the complexity requirement. Passwords that do not meet both standards are vulnerable to so-called "brute force attack," in which unauthorized individuals repeatedly try to guess the password. A successful brute force attack would open access to the application and the information it contains. DSNY officials stated that they are aware of the situation and are planning to implement the required controls by July 1, 2019.

## Three Critical Applications Did Not Lock the Account after Five Failed Login Attempts

DoITT's *Password Policy* states that all accounts that provide access to sensitive, private, or confidential information "must be automatically disabled after a maximum of five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes." However three of DSNY's critical applications did not comply with the abovementioned policy's account-lockout requirement after five failed login attempts.

During our system test of six critical applications, we entered the wrong password several times into the abovementioned applications' password fields. After five failed consecutive attempts, we entered the correct password on the sixth attempt and were able to logon to the applications. Hence, the applications do not properly lock the account after five failed login attempts. Allowing numerous failed login attempts increases the possibility of an unauthorized person's correctly guessing the password, and the risk that confidential or personal information collected and stored in the application could be exposed to intruders. DSNY informed us that the necessary work to address the issues for one application would be completed by July 1, 2019. As of February 15, 2019, DSNY has addressed the issues for the other two applications.

## Recommendations

DSNY should:

1. Immediately disable former and inactive employees' user accounts in all of its applications and implement procedures to ensure that going forward frequent periodic reviews are conducted to promptly identify and disable the application user accounts of former and inactive employees.

   ***DSNY Response:*** "We agree that terminating the access of former and on-leave employees is necessary for the security of sensitive data stored in DSNY applications. We note that the 'inactive' employees list received from PMS contained some active users, and that pursuant to DSNY off-boarding procedures the passwords on some of the active user accounts had been changed when the employee left DSNY or went on long-term leave. For these reasons, we believe the number of active accounts accessible by former or on-leave employees to be less than 583."

[8] A system test was performed on 6 out of 10 critical applications.

***Auditor Comment:*** As stated above, we compared the lists of active user accounts for five critical applications against a list of inactive employees from PMS and found that 583 former employees or employees on long-term leave in PMS are listed as active in the multiple lists provided by DSNY. We provided the results of this comparison to DSNY. At the exit conference, DSNY officials stated that there were extenuating circumstances why inactive employees would be on the active employee list. However, DSNY did not provide supporting and verifiable documentation that would evidence why inactive employees were listed as active employees.

2. Remove all generic logins from its application and replace them with unique user logins, each of which identifies and is issued only to an individual employee or other authorized user.

   ***DSNY Response:*** "We agree with the auditor's assessment, and the remediation timeline indicated in the auditor's report is correct."

3. Update the three applications to comply with DoITT's 90-day password expiration requirement.

   ***DSNY Response:*** "We agree with the auditor's assessment, and the remediation timeline indicated in the auditor's report for the [redacted] and [redacted] applications is correct.

   The [redacted] application interfaces with the [redacted] application owned by the Department of Citywide Administrative Services (DCAS). Replacement of [redacted] requires coordination with DCAS, and a replacement date has not yet been agreed to."

4. Comply with DoITT's *Password Policy* to ensure that passwords that provide access to its applications meet the prescribed standards for length (minimum-number-of characters) and complexity.

   ***DSNY Response:*** "Since the audit began, [redacted] have been remediated to meet DoITT's password minimum length and complexity requirements. We are actively working to remediate the [redacted] application by July 1, 2019."

5. In accordance with DoITT standards, ensure that user accounts are locked and remain locked for a minimum of 15 minutes after five sequential invalid login attempts.

   ***DSNY Response:*** DSNY agreed with the recommendation.

# Application Security Weaknesses

## An Application's Hand-Held Terminals Used Outdated, Unsupported Hardware and Software

An application allows sanitation officers in the field to use hand-held, printer-equipped computers to issue summonses for sanitation code violations, such as noncompliance with laws that govern the maintenance of clean streets, prohibit illegal dumping, and require the proper storage and disposal of waste and recyclable materials. However, the application's hand-held devices used

outdated and unsupported hardware and software, which poses a security risk, as explained below.[9]

During the application system walkthrough, we asked DSNY officials about the hardware and software used for their hand-held devices. DSNY explained that the 409 hand-held devices currently being used by sanitation officers are no longer manufactured and that the agency replaces broken units with refurbished ones it purchased as needed. DSNY also informed us that the hand-held devices operating system is no longer supported. Unsupported products no longer receive software updates, security patches, and fixes to keep the product functioning. Software updates, patches, and fixes are necessary because they address vulnerabilities and help prevent cyberattacks.

Initially, DSNY stated that it had no plans to upgrade the application's hardware and software, but in response to our follow-up inquiry, the agency provided new information, specifically, that it was in the process of upgrading the application and the old hand-held devices. Our review of the new information revealed that DSNY had purchased 400 new hand-held devices in July 2017. DSNY explained that the new hand-held devices featured a more secure and supported operating system and hardware. However, out of the 400 new hand-held devices—4 were in the field and 70 were assigned to borough offices. Meanwhile, the old hand-held devices remain in use in the field. DSNY stated that the outdated hand-held device hardware will no longer be used after May 2019. Moreover, after the exit conference DSNY stated that 114 of the new hand-held devices are in use on four sites and that the majority of summonses are issued with the new hand-held devices.

## Hand-Held Terminals Stored Public and Private Information Unencrypted in a Removable Memory Card

DoITT's *Portable Data Security Policy* states, "All portable computing devices used to process and store City of New York information must be physically protected and appropriate security measures provided for the data contained." Further, the policy states, "Confidential information can be stored on removable media (e.g., disks, removable drives, tapes, flash memory cards, CDs, USB memory devices) if the data is encrypted." However, the information stored in the old hand-held devices removable memory cards was not encrypted.

During our application walkthrough and follow-up meeting, DSNY officials stated that the information stored in the old hand-held devices memory card is not encrypted. The hand-held devices memory card contains application code, a database with a list of users assigned to the hand-held devices, their digital signatures, information regarding regulations, the names and addresses of repeat offenders, and data for all summonses that the hand-held device containing the memory card issued on that particular day.[10]

DSNY officials explained that specific software is needed to be able to read the information stored in the old hand-held devices memory card. Nevertheless, the possibility exists that an unauthorized person could obtain the software needed to access the information stored in the memory card if the device is lost or stolen. As noted previously, DSNY informed us that it plans to discontinue all use of the old hand-held devices as of the end of May 2019.

[9] The application security weaknesses listed below do not affect the functionality of the application or the validity and integrity of any issued summonses.

[10] While in use at the field, the hand-held device stores issued summons data in the memory card. Once the hand-held device is docked at the office the data is transferred to the application SQL server database and then copied to other locations.

## Recommendations

DSNY should:

6. Complete the roll-out of the new hand-held devices and decommission all old ones, as planned, to address the security risks posed by the use of outdated and unsupported hardware and software from the old hand-held devices in use as of the date of this report.

   ***DSNY Response:*** "As correctly stated in the audit report, at the time of the exit conference, DSNY possessed 400 new HHTs, out of which 114 were in use on four sites, and the majority of summonses were (and continue to be) issued with the new hand held devices. Since the audit report was drafted, DSNY has increased the number of HHT devices in use to 174. We continue to expect that the old HHT hardware will be discontinued after May 2019."

7. Ensure that data encryption and security features are enabled in all new hand-held devices to protect the data they store and transmit.

   ***DSNY Response:*** "DSNY is committed to meeting all applicable security standards. As outlined below, we believe that, arguably, the information stored on the old HHT memory cards is not confidential information, and as such encryption is not required under DoITT's Portable Data Security Policy.

   The auditor's response indicates that the old HHT memory card contains 'application code, a database with a list of users assigned to the HHTs, their digital signatures, information regarding regulations, the names and addresses of repeat offenders, and data for all summonses that the HHT containing the memory card issued on that particular day.' The HHT memory card does not contain application code. While digital signatures do exist on the cards, their use was discontinued. The remaining data on the memory card includes information regarding HHT users, regulations, repeat offenders, and summonses, all of which we believe to be public information.

   As an additional security feature, the new HHTs can only communicate with the DSNY network if plugged into a valid cradle in at the location to which the device is assigned. DSNY does not activate the generic 'security features enabled' setting on the new HHT devices as we have confirmed with Microsoft that anti-virus software is not available for hand held devices. To access data stored on a device, a malicious actor would need both physical access to the HHT itself and the correlating 'cradle' in order to overcome the device's security features."

   ***Auditor Comment:*** DSNY states that hand-held devices memory card "arguably" does not contain confidential information, therefore it is not required to encrypt the data. However, DSNY provided a database table that details the data stored in the memory card. The table includes configuration data which, if not protected, could lead to possible security breaches. Moreover, in its response DSNY states that the additional security features in the new hand-held devices operating system do not need to be enabled because physical access to the hand-held devices and cradle is needed in order to access the data. However, the possibility exists that a malicious actor could gain access to both the hand-held device and cradle and access the data because the security features, like encryption and secure boot, are not enabled. Therefore, we urge DSNY to implement this recommendation.

# Lack of Protection for Transmitted and Stored Data

## Two Critical Applications, and Two Non-Critical Applications, Used an Unsecured Network Protocol

According to DoITT's *Encryption Policy*, "All City of New York data with a classification of private or confidential may not be stored and/or transmitted across any communication mechanism unless it is protected using approved encryption technology." DoITT's *Encryption Standard* lists HTTPS as a supported, secure, alternative network protocol to the HTTP protocol for transmitting private or confidential information. Separately, DoITT's *Application Security Policy* states, "Protecting data's confidentiality, integrity, and availability is a principle that must be maintained at all times. Proper encryption solutions must be implemented to protect data at rest, in use or in motion." However, four DSNY applications do not protect data in motion.

During application walkthroughs of 10 critical and 10 non-critical applications, and system tests of 6 critical applications, we determined that DSNY implemented 2 critical and 2 non-critical web-based applications that use an unsecured communications protocol, HTTP, which does not comply with DoITT's policies and standard. The HTTPS encrypted protocol ensures that transmitted data and messages can be read by only the two parties involved in the conversation. An unsecured protocol does not provide that protection and potentially could allow the communication to be intercepted and read by an unauthorized individual. DSNY applications should use the secure HTTPS protocol. In our follow-up communications regarding this issue, as of February 15, 2019, DSNY stated that it had implemented the required change for three applications. Further, according to DSNY, the fourth application will be replaced. However, DSNY did not provide a replacement date. Until the application is updated to the secure protocol, it poses the risk of having an unauthorized user gaining access and reading the data.

## One Application Failed to Protect DSNY's Scanned Documents with Encryption

As noted above, DoITT's *Application Security Policy* requires proper encryption solutions to protect data at rest, in use, or in motion. However, during the application walkthroughs of 10 critical and 10 non-critical applications, we found that a DSNY application was noncompliant in that it stored and accessed approximately six million scanned documents that currently are not encrypted. The use and storage of unencrypted scanned documents could lead to the improper exposure, theft, modification, or deletion of the data they contain. In our discussion of this issue, DSNY explained that its application team plans to encrypt existing and future documents and that it expected the encryption project to start in March 2019 with a duration of 12 to 18 months, depending on resource availability. As of the date of this draft report DSNY has not started the encryption project to protect its scanned documents.

## Recommendations

DSNY should:

8. Ensure all web-based applications utilize the secure HTTPS protocol.

   ***DSNY Response:*** "As noted in the Auditor's report, we have remediated the [redacted] applications.

[redacted] application interfaces with the [redacted] application owned by the Department of Citywide Administrative Services (DCAS). Replacement of [redacted] requires coordination with DCAS, and a replacement date has not yet been agreed to"

9. Ensure all scanned documents are protected with encryption.

   ***DSNY Response:*** "Contrary to the audit finding, as of the date of the auditor's report DSNY had started the [redacted] encryption project. (In fact, the 12 to 18 month duration estimate itself evidences discussions and a project plan). To date, the [redacted] application has been moved to the cloud, and we are actively working to upgrade the application, both of which are prerequisites to enabling encryption of existing and future documents stored in [redacted]. The 12 to 18 month estimate, with a start in March 2019, remains accurate."

   ***Auditor Comment:*** On February 8, 2019 DSNY stated that the project had not started yet, and that the delay was due to technical issue with overall solution implementation. DSNY also informed us, as stated in the report section above, that the tentative project timeline is 12-18 months starting in March 2019. However, DSNY did not confirm the start of the encryption project as of the date the draft report was issued.

# Vulnerability Management Program Shows Deficiencies

## DSNY Has Not Conducted Application Vulnerability Scans on Three Critical Applications

DoITT's *Vulnerability Management Policy* states, in part, "All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." The policy further states that "[v]ulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation." To assess DSNY's vulnerability management program, we requested application vulnerability scans for all critical applications. However, the agency did not provide vulnerability scans for three critical applications.

Information security involves an ongoing process of finding and addressing security gaps, including by periodically performing vulnerability scans. Open vulnerabilities must be resolved rapidly to prevent attackers from exploiting them to access sensitive and confidential information and possibly degrading system operations and damaging data. In response to our finding DSNY tentatively scheduled vulnerability scans of the three abovementioned applications as follows: two applications' vulnerability scans are in progress with target dates of February 1 and 15, 2019 respectively; a third application's vulnerability scan is scheduled for the week of May 6, 2019.

## DSNY's Network Vulnerability Scan Reports Were Unreliable

NIST Special Publication 800-53 states, "Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations." The publication further explains that correlating the results of multiple monitoring tools helps an organization to build, operate, and maintain effective monitoring tools:

> The organization correlates information from monitoring tools employed throughout the information system. . . . Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs.

However, DSNY did not ensure that its network vulnerability tool operates correctly. As part of the audit, we asked DSNY to provide us with network scan reports. In response, the agency provided a network scan report from June 6, 2018, which revealed several vulnerabilities. We informed DSNY of the vulnerabilities identified in the report and later asked for a new network scan report to determine whether the initial vulnerabilities were addressed. DSNY thereafter provided us with two additional network scan reports dated July 13, and 24, 2018, respectively, which showed the same vulnerabilities as had been revealed by the June 6, 2018 report—vulnerabilities that the agency claimed it had addressed. DSNY officials stated that they have been working with DoITT to resolve these issues and informed us that the scan reports were unreliable. Unreliable vulnerability scan reports prevent the agency from knowing about the weaknesses in the network or confirming the success of efforts to remove the vulnerabilities. Such knowledge is essential to enable the agency to resolve weaknesses that could allow a malicious actor to gain access to computers and data and, for example, steal data, or initiate a ransomware attack that could disable the agency's computers and cut off its access to the data it needs to operate.

On December 28, 2018 DSNY informed that the issue with the network scan reports has been resolved and provided us with three new consecutive network scans that showed that the agency had addressed the previously-found vulnerabilities. However, the three new reports showed that several DSNY computers were using an outdated operating system, which pose new previously unidentified vulnerabilities and place the network infrastructure at risk. We asked DSNY about the new vulnerabilities and, as of February 15, 2019, the agency responded that it has removed the machines with the outdated operating system from its network. However, DSNY did not provide a follow up vulnerability scan report to confirm that the vulnerabilities were addressed

## Recommendations

DSNY should:

10. Periodically conduct necessary vulnerability scans of critical applications, address any vulnerabilities found, and conduct a follow up scan to confirm vulnerability remediation, as directed in DoITT's *Vulnerability Management Policy*.

    ***DSNY Response:*** "As a New York City agency, DSNY relies on DoITT and NYC3 to monitor for system vulnerabilities. We provided system scans at the auditor's request, however we rely on DoITT to maintain a vulnerability management program and process."

    ***Auditor Comment:*** Although DSNY relies on DoITT to conduct vulnerability scans, DSNY is responsible for its applications' vulnerability management. Therefore we reiterate our recommendation to periodically conduct necessary vulnerability scans of critical applications, address any vulnerabilities found, and conduct a follow up scan to confirm vulnerability remediation.

11. Test all vulnerability scanning tools to assess the reliability of the scanning results, and correlate the results from vulnerability scanning tools with the output of other security tools, as recommended by the National Institute for Standards and Technology (NIST).

    ***DSNY Response:*** "As a New York City agency, DSNY is mandated to use the network vulnerability tools and associated scan reports selected, owned, and maintained by DoITT and NYC3. As such, it is not possible for DSNY to ensure that the network vulnerability tool operates correctly, or that the scans are accurate. As noted, we can, and do, work with DoITT and NYC3 to resolve tool or report issues when we become aware of them. In some cases it may not be clear to DSNY that a tool output or scan report is not accurate or reliable.

    Will request a vulnerability scan from DoITT and NYC3 to confirm that the risk posed by computers with outdated operating system no longer exists following the removal of the computers."

    ***Auditor Comment:*** Although DSNY uses the network vulnerability tools owned and maintained by DoITT, DSNY is responsible for ensuring that the scan report generated is reviewed, vulnerabilities are addressed and a follow-up report is obtained to confirm remediation efforts. By remediating found vulnerabilities and reviewing follow-up scan reports, DSNY ensures, in some cases, that the network vulnerability tool is operating correctly.

## Pending Risk Assessment Report Recommendations

To determine its security posture, DSNY requested a security program assessment from a third-party vendor and obtained the vendor's report on July 1, 2016. However, DSNY has not implemented one and has partially implemented four recommendations made on the report. In addition, DSNY has not addressed one additional observation made on the report. Consequently, the agency remains noncompliant with applicable DoITT policies in areas such as: (1) a data classification program; (2) a Software Development Life Cycle (SDLC) process that identifies and remediates vulnerabilities; (3) a security training and awareness program; and (4) a disaster recovery plan to address the effects of a potential agency-wide disruptive cyber event. The relevant DoITT policies are as follows:

- DoITT's *Data Classification Policy*, which states, "All information at the City of New York and corresponding agencies will be classified at one of four levels; public, sensitive, private, or confidential." Data classification allows an agency to protect the data based on its classification; without classifying its data, DSNY is unable to determine how to adequately protect it.

- DoITT's *Citywide Application Security Policy* states, in part "Modifications of the application must go through a change release process that includes an appropriate security assessment." The policy further states that "Releases to a production environment are approved based on the vulnerabilities found during the security assessment." Part of an SDLC process entails testing for vulnerabilities during the development phase and after the application is implemented. DSNY did not provide vulnerability scans for three critical applications as mentioned in the report section where vulnerability management deficiencies are discussed.

- DoITT's *Citywide Information Security Policy, CISO* Role states, "Establishing an information technology security awareness program to ensure all department employees

understand and adhere to information technology policies and standards." A security training and awareness program is designed to reduce the number of security breaches that occur through a lack of employee security awareness. Routine, ongoing training must be provided to all employees to inform them how to recognize potential threats and how they should respond to protect the agency. Although, DSNY has not conducted a security training and awareness program, it is currently working with NYC Cyber Command (NYC3) to conduct periodic security awareness campaigns and training.[11]

- DoITT's *Citywide Application Security Policy* states, in part, "Application business owners must ensure that each application has a defined Business Continuity Plan and a Disaster Recovery Plan to ensure its readiness to respond to events that could disrupt the application's service continuity." Although, DSNY has disaster recovery procedures for various scenarios, it has not developed a disaster recovery procedure for a full-blown security event. Until the agency fully prepares for a large, agency-wide cyber-attack, it will not know its recovery capabilities, the resources it needs, and how long it will take to achieve full recovery of its systems and data. The absence of such a disaster recovery plan places DSNY's IT infrastructure resiliency in an uncertain state.

The abovementioned July 1, 2016 security program assessment report made seven recommendations that had a two-year roadmap for implementation (July 1, 2016 to July 1, 2018), and included several observations relating to security areas. As of December 2018, DSNY had implemented two of these recommendations, had not implemented one, and had partially implemented the remaining four. In addition, DSNY had not addressed one finding mentioned in the observations section of the report.

Specifically, DSNY had not fully implemented the following five recommendations (one not implemented and four partially implemented): a security governance program; an assessment of current skills; a data classification program; an SDLC process to identify and remediate vulnerabilities in DSNY applications; and a security training and awareness program. And the agency had not addressed a separate observation in the report—the lack of a disaster recovery plan to address an agency-wide disruptive cyber event. After we discussed this finding with DSNY officials during the audit, the agency reported taking additional action; specifically, on February 15, 2019, DSNY informed us that the SDLC process has been integrated into the work of its project management office, and that DSNY is currently working with NYC3 to conduct vulnerability scans. The agency also stated that it is ready to conduct NYC3-provided security awareness training but is waiting for NYC3 to start the training campaign. DSNY further informed us that NYC3 has taken the lead on a Citywide data classification project and will provide a Citywide solution that DSNY will leverage to address the need. In addition, DSNY stated that it will take an additional two years to fully implement the remaining recommendations due to resource constraints.

## Recommendation

DSNY should:

12. Ensure that the recommendations made in the 2016 security assessment report are implemented.

[11] The New York City Cyber Command (NYC3), established in July 2017, is charged with setting citywide cybersecurity policies, directing response to cyber incidents, and advising City Hall and more than 100 agencies on the City's overall cyber defense.

***DSNY Response:*** "We address each of the security assessment items here. The actions referred to below were taken by DSNY prior to the start of the current audit." [see the addendum to this report for the agency's full response]

***Auditor Comment:*** As stated above, as of the date the draft report was issued, DSNY had not fully implemented five recommendations from the 2016 security assessment report. As of February 15, 2019, DSNY estimated that it will take an additional 1-2 years to implement those recommendations. Therefore, we reiterate our recommendation to ensure that the recommendations made in the 2016 security assessment report are implemented.

# DETAILED SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

The scope of this audit was from March 2018 through November 2018. To achieve the audit objectives we:

- Reviewed DoITT's security policies and standards to determine current security policies in place that apply to City agencies.
- Reviewed NIST Special Publications 800-53 and 800-137 to determine best practice guidelines for security controls.
- Reviewed DSNY's 2016 response to Comptroller's Directive #1, to determine DSNY's information technology status and application environment.
- Reviewed DSNY's 2016 Strategic Plan to determine the agency's current goals, objectives, and priorities.
- Requested and reviewed organization charts for the agency overall and the agency units responsible for DSNY's information security to determine the organizational unit in charge of information security.
- Requested and reviewed policies, procedures, standards, strategic plans, best practices guides and change management controls for DSNY's information security to determine the security controls implemented to protect information systems and data.
- Requested and reviewed DSNY's detailed network diagrams showing critical systems and information security controls to determine the presence of information security controls to safeguard critical systems and data.
- Requested and reviewed DSNY's detailed technical information for information system hardware, software, user devices, and server/data-room devices to determine information security controls in place at the workstation, server, user-devices, and software levels to protect the systems and data.
- Requested and reviewed DSNY's last information security audit, assessments reports, and results to determine information security controls implementation and performance.
- Requested a list of all DSNY applications. DSNY provided a list of 136 applications of which only 10 were critical. We conducted walkthroughs of all critical applications and 10 randomly selected non-critical applications to determine whether the selected applications have controls in place to safeguard the system and data. During our walkthroughs with DSNY we were also able to observe the encryption and whether the applications use the secure or unsecured network protocol. Our observations were confirmed by DSNY during the walkthroughs and in follow-up emails.

- Requested and reviewed DSNY's specific access and security controls in place to prevent unauthorized access to critical applications and systems to determine the adequacy of the controls.
- Requested and reviewed DSNY's information on the following security processes to determine the presence and maturity of specific information security controls: patch management (change management process), malware management (incident reports), asset management tools, virus management (incident response procedures), advanced persistent threat management procedures, privileged user management procedures, data loss/leak/exfiltration/corruption management tools, mobile device management applications, wireless access management controls, network access management controls, backup/restore data management procedures, password management procedures, and physical security management procedures.
- Requested and reviewed DSNY's hardware, software, network diagram, service level agreement (including third party services) for the following information security systems to determine their implementation and effectiveness: intrusion prevention systems, intrusion detection systems, security information event management systems, managed information security services, list of staff in charge of installation, operation, patching, and monitoring the above systems.
- Requested and reviewed DSNY's hardening procedures (procedures to increase the security, to make the system more resilient against attacks) applied to workstations, servers, applications, network devices, data storage devices, host machines, and virtual machines to determine controls in place to protect the information systems and data.
- Requested and reviewed DSNY's last business continuity/disaster recovery exercise report to determine the effectiveness and maturity of such controls.
- Requested and reviewed DSNY's last data backup/restore exercise report to determine effectiveness and maturity of security controls.
- Requested and analyzed user lists for five out of 10 DSNY's critical applications to determine whether user lists of active staff contain inactive staff that should not have access to the applications. We compared the provided user account lists against City payroll database data.
- Requested read-only access and tested six out of 10 DSNY's critical applications to determine whether the applications follow password and other security policies. We tested compliance to DSNY's and DoITT's applicable security policies. Conducted access control tests such as password format, length and complexity. Performed tests to determine whether DSNY disables users after five sequential invalid login attempts within a 15-minute period, and has a lock-out feature after 15 minutes of inactivity.
- Requested and reviewed a list of all mobile devices including the HHTs to determine the number of HHTs being used by DSNY.
- Requested and reviewed application documentation to determine how the data is protected in the HHTs removable memory card.
- Requested and reviewed DSNY's application vulnerability reports for all critical applications to determine the security posture of each application. We also requested follow-up application vulnerability reports to determine whether previously detected vulnerabilities have been addressed.

- Requested and reviewed DSNY's network vulnerability reports to determine the network security posture. We requested a follow-up network vulnerability report to determine whether previously detected vulnerabilities have been addressed.

The results of the above tests, while not projectable to their respective populations, provided a reasonable basis for us to evaluate and support our conclusions about DSNY implementation of security controls to protect its systems and data.

# sanitation

**Kathryn Garcia** Commissioner

**Steven Costas**
**Acting Commissioner**

125 Worth Street
Room 717
New York, NY 10013
Scostas@dsny.nyc.gov
646-885-4727

March 29, 2019

Ms. Marjorie Landa
Deputy Comptroller for Audits
One Centre Street, Room 1100
New York, NY 10007

Re: Audit Report on the Security Controls at the NYC Department of Sanitation over its Computer Systems (Audit Number SI18-115A), dated March 15, 2019.

Dear Deputy Comptroller Landa,

Thank you for the opportunity to review and comment on the above referenced audit report which highlighted five (5) major areas of concern. We have attached our responses to each of twelve findings and recommendations outlined in your draft report on the Department of Sanitation's Security Controls over its Computer Systems. We request that you take our comments into serious consideration and reflect them in the final audit report.

Sincerely,

Steven Costas
Acting Commissioner

DSNY has reviewed the Draft Report on the Security Controls at the New York City Department of Sanitation Over its Computer Systems, Audit #SI18-115A, dated March 15, 2019. The audit report identified weaknesses that need to be addressed to protect the information in DSNY's computerized environment. We will continue working to improve our system security and access controls and to incorporate your recommendations where practical. Our responses to your specific findings and recommendations are outlined below.

## *Access Control Weaknesses*

***Finding # 1***

***Risk of Unauthorized Access to DSNY's Computer Applications through Active User Accounts Assigned to Former or On-leave Employees***

*The auditor's report states, in relevant part:*

*DoITT's Identity Management Security Policy states, "User accounts will be created and de-provisioned in a timely manner." However, DSNY did not ensure that its user accounts for five critical applications [redacted] were promptly deactivated for 583 former employees and other inactive users, such as employees on long-term leave.*

*We compared DSNY's lists of active user accounts for five critical applications as of June 29, 2018 against a list of inactive employees from the City's Payroll Management Systems (PMS) and found that 583 former employees or employees on long-term leave in PMS are listed as active in the multiple user lists provided. . . .*

*DSNY officials informed us that the agency disabled the accounts after we brought the issue to their attention, stating, "The Active Directory accounts that were questionable were investigated/disabled and moved to a departed user OU [organizational unit] . . . . The process going forward is being handled via a new off boarding method that will inform IT of departing users and kick off a process to remove accounts and access."*

***Recommendation # 1***

*DSNY should immediately disable former and inactive employees' user accounts in all of its applications and implement procedures to ensure that going forward frequent periodic reviews are conducted to promptly identify and disable the application user accounts of former and inactive employees.*

**Agency Response # 1**

We agree that terminating the access of former and on-leave employees is necessary for the security of sensitive data stored in DSNY applications. We note that the "inactive" employees list received from PMS contained some active users, and that pursuant to DSNY off-boarding procedures (see below) the passwords on some of the active user accounts had been changed when the employee left DSNY or went on long-term leave. For these reasons, we believe the number of active accounts accessible by former or on-leave employees to be less than 583.

DSNY off-boarding procedures allow for managers to request, and receive, access to the account of a former or on-leave employee for business continuity purposes. In these cases, the relevant account password is changed before the account is made accessible to the manager. DSNY's new off-boarding procedures leaves this process in place, and now limits the amount of time that accounts reassigned to managers of former or on-leave employees may remain active before being disabled.

The Auditor's report states that the new off-boarding method will "inform IT of departing users and kick off a process to remove accounts and access." For clarity, the current and new off-boarding procedure relies on the DSNY Human Resource Unit to provide notice to IT when an employee's status is expected to change. DSNY IT is working with Human Resources to implement policies and procedures ensuring such notification is timely. As an additional checkpoint, DSNY is working to generate a report (due Q4 of 2019) of employees whose status has changed in the NYC Automated Personnel System (NYCAPS). Off-boarding procedures will include periodic review of this report to ensure that accounts of inactive or on-leave employees have been properly reassigned or deactivated.

***Finding # 2***

***One Critical Application Allows the Use of Generic Login IDs***

*DoITT's Application Security Policy states, "All access to City of New York systems must be authorized and based on individual identification and authentication." However, DSNY's [redacted] application does not comply with DoITT policy in that it has 95 generic login IDs that do not identify a specific individual.[9] During our analysis of active user accounts for critical applications described in the previous section, we found that the [redacted] application uses generic login IDs. While a regular user ID identifies and is used by a single employee, a generic login ID can be assigned to multiple employees. For example, a mechanic in a sanitation garage may be assigned a generic login that identifies his or her role and location. The mechanic working the next shift in the same garage will use the same generic login ID.*

*DSNY explained that there is an operational need for generic login IDs, since the agency assigns and moves personnel quickly, as needed, during periods of heavy demand for staff. To avoid the delay that would result if it had to obtain new credentials when it moves staff who need to access the [redacted] application, the agency relies on generic login IDs. However, having multiple users using the .same generic login ID makes it difficult to identify or track the individuals who make specific changes to the application's data. Thus, generic login IDs create a lack of accountability and a gap in the audit trail which is a critical control over the system. In response to our raising this issue, DSNY officials stated that they plan to switch the current local login/authentication method for [redacted] to a different method-one that leverages the DSNY Active Directory/ Lightweight Directory Access Protocol (LDAP) as an additional level of user-identification and authentication, and thereby endeavor to restore accountability to the continued use of generic login IDs for [redacted] access.[10] The agency also stated that the work required to make that change is expected to start mid-April 2019 and end by December 2019.*

***Recommendation # 2***

*DSNY should remove all generic logins from its application and replace them with unique user*

*logins, each of which identifies and is issued only to an individual employee or other authorized user.*

**Agency Response # 2**

We agree with the auditor's assessment, and the remediation timeline indicated in the auditor's report is correct. In addition, DSNY has implemented [redacted] for not only Multi Factor Authentication, but also for the ability to manage and control generic logins which would allow DSNY to identify who used the generic login and when.

***Finding # 3***

***Three Applications Did Not Require User Passwords to Expire after 90 Days***

*DoITT's Password Policy states, "User Account passwords and/or PINs must expire at least every 90 days." However, we found that three of DSNY's applications [redacted] do not comply with DoITT's 90-day password-expiration rule. Having application passwords change periodically lowers the risk that unauthorized users have ample time to guess a password and gain access to the application and its data.*

*During walkthroughs of 10 critical and 10 non-critical applications, DSNY officials stated that the three abovementioned applications' passwords are not set to expire after 90 days. DSNY informed us that it plans to upgrade the [redacted] application by June 2019 and that the upgrade should make that application compliant with the 90-day password expiration policy. As for the [redacted] application, as mentioned above, DSNY plans to switch from generic logins to Active Directory/LDAP logins, which, if accomplished, would make the application compliant with the password expiration policy. Finally, DSNY officials stated that they have no plan to implement the 90-day password expiration rule in [redacted] application, since the agency plans to replace it. However, DSNY did not provide a replacement date. Until the three abovementioned applications are made to comply with the 90-day password expiration rule, the applications remain at risk of unauthorized users gaining access to the application and its data.*

***Recommendation # 3***

*DSNY should update the [redacted] applications to comply with DoITT's 90-day password expiration requirement.*

**Agency Response # 3**

We agree with the auditor's assessment, and the remediation timeline indicated in the auditor's report for the [redacted] applications is correct.

[redacted] application interfaces with the [redacted] application owned by the Department of Citywide Administrative Services (DCAS). Replacement of [redacted] requires coordination with DCAS, and a replacement date has not yet been agreed to.

***Finding # 4***

***Three Critical Applications Did Not Comply with City Requirements for Password Minimum Length and/or Complexity***

*DoITT's Password Policy states that passwords and PINs must have a minimum length of eight characters and must contain at least one alphabetic character and at least one numeric character or special character, such as an exclamation point, a number sign, or a dollar sign among others. Similarly, DSNY's Password Policy states that strong passwords contain at least eight characters in length, both upper and lower case characters, and have digits and special/punctuation characters. However, three of DSNY critical applications [redacted] did not comply with one or both requirements-for password-length and complexity-set forth in DoITT's and DSNY's password policies.*

*During our system test of critical applications, we found that [redacted] applications failed to meet the password minimum-length standard required by DoITT's and DSNY's policies.[11] In addition, [redacted] did not meet the complexity requirement. Passwords that do not meet both standards are vulnerable to so-called "brute force attack," in which unauthorized individuals repeatedly try to guess the password. A successful brute force attack would open access to the application and the information it contains. DSNY officials stated that they are aware of the situation and are planning to implement the required controls by July 1, 2019.*

***Recommendation # 4***

*DSNY should comply with DoITT's Password Policy to ensure that passwords that provide access to its applications meet the prescribed standards for length (minimum-number-of characters) and complexity.*

**Agency Response # 4**

Since the audit began, [redacted] have been remediated to meet DoITT's password minimum length and complexity requirements. We are actively working to remediate the [redacted] application by July 1, 2019.

***Finding # 5***

***Three Critical Applications Did Not Lock the Account after Five Failed Login Attempts***

*DoITT's Password Policy states that all accounts that provide access to sensitive, private, or confidential information "must be automatically disabled after a maximum of five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes." However three of DSNY's critical applications [redacted] did not comply with the abovementioned policy's account-lockout requirement after five failed login attempts.*

*During our system test of six critical applications, we entered the wrong password several times*

*into the abovementioned applications' password fields. After five failed consecutive attempts, we entered the correct password on the sixth attempt and were able to logon to the applications. Hence, the applications do not properly lock the account after five failed login attempts. Allowing numerous failed login attempts increases the possibility of an unauthorized person's correctly guessing the password, and the risk that confidential or personal information collected and stored in the application could be exposed to intruders. DSNY informed us that the necessary work to address the issues would be completed by July 1, 2019 for [redacted]. As of February 15, 2019, DSNY has addressed the issues for the [redacted] applications.*

***Recommendation # 5***

*DSNY should, in accordance with DoITT standards, ensure that user accounts are locked and remain locked for a minimum of 15 minutes after five sequential invalid login attempts.*

**Agency Response # 5**

We agree with the auditor's assessment, and as noted in the auditor's report we have remediated the [redacted] applications, and plan to complete the [redacted] remediation by July 1, 2019.

## *Application Security Weaknesses*

***Finding # 6***

***The [redacted] Application Hand Held Terminals Used Outdated, Unsupported Hardware and Software***

*The [redacted] application allows sanitation officers in the field to use handheld, printer-equipped computers to issue summonses for sanitation code violations, such as noncompliance with laws that govern the maintenance of clean streets, prohibit illegal dumping, and require the proper storage and disposal of waste and recyclable materials. However, the [redacted] HHT used outdated and unsupported hardware and software, which poses a security risk, as explained below*[12]

*During the [redacted] system walkthrough, we asked DSNY officials about the hardware and software used for their HHTs. DSNY explained that the 409 HHTs currently being used by Sanitation officers are no longer manufactured and that the agency replaces broken units with refurbished ones it purchased as needed. DSNY also informed us that the HHTs' operating system is no longer supported. Unsupported products no longer receive software updates, security patches, and fixes to keep the product functioning. Software updates, patches and fixes are necessary because they address vulnerabilities and help prevent cyber-attacks.*

*Initially, DSNY stated that it had no plans to upgrade the [redacted] hardware and software, but in response to our follow-up inquiry, the agency provided new information, specifically, that it was in the process of upgrading the [redacted] application and the old HHTs. Our review of the new information revealed that DSNY had purchased 400 new HHTs in July 2017. DSNY explained that the new HHT devices featured a more secure and supported operating system and*

*hardware. However, out of the 400 new HHTs-4 were in the field and 70 were assigned to borough offices. Meanwhile, the old HHTs remain in use in the field. DSNY stated that the outdated HHT hardware will no longer be used after May 2019. Moreover, after the exit conference DSNY stated that 114 of the new HHTs are in use on four sites and that the majority of summonses are issued with the new hand held terminals.*

***Recommendation # 6***

*DSNY should complete the roll-out of the new [redacted] HHTs and decommission all old [redacted] HHTs, as planned, to address the security risks posed by the use of outdated and unsupported hardware and software from the old HHTs in use as of the date of this report.*

**Agency Response # 6**

The auditor's report points to a miscommunication, during the audit, between the auditor and a DSNY developer as to the state of the [redacted] application and hardware upgrade. To remove any confusion, before the audit began, DSNY had been actively working to upgrade the [redacted] software and deploy the new HHT devices. At the time of the audit, a vendor contract for the rewrite of the [redacted] application was in place, and the vendor had begun work along with internal DSNY resources.

As correctly stated in the audit report, at the time of the exit conference, DSNY possessed 400 new HHTs, out of which 114 were in use on four sites, and the majority of summonses were (and continue to be) issued with the new hand held devices. Since the audit report was drafted, DSNY has increased the number of HHT devices in use to 174. We continue to expect that the old HHT hardware will be discontinued after May 2019.

***Finding # 7***

***[redacted] Hand Held Terminals Stored Public and Private Information Unencrypted in a Removable Memory Card***

*DoITT's Portable Data Security Policy states, "All portable computing devices used to process and store City of New York information must be physically protected and appropriate security measures provided for the data contained." Further, the policy states, "Confidential information can be stored on removable media (e.g., disks, removable drives, tapes, flash memory cards, CDs, USB memory devices) if the data is encrypted." However, the information stored in the old [redacted] HHTs' removable memory cards was not encrypted.*

*During our [redacted] walkthrough and follow-up meeting, DSNY officials stated that the information stored in the old HHT's memory card is not encrypted. The HHT's memory card contains application code, a database with a list of users assigned to the HHTs, their digital signatures, information regarding regulations, the names and addresses of repeat offenders, and data for all summonses that the HHT containing the memory card issued on that particular day.*[13]

*DSNY officials explained that specific software is needed to be able to read the information stored in the old HHT's memory card. Nevertheless, the possibility exists that an unauthorized*

*person could obtain the software needed to access the information stored in the memory card if the device is lost or stolen. As noted previously, DSNY informed us that it plans to discontinue all use of the old HHTs as of the end of May 2019.*

***Recommendation # 7***

*DSNY should ensure that data encryption and security features are enabled in all new [redacted] HHTs to protect the data they store and transmit.*

**Agency Response # 7**

DSNY is committed to meeting all applicable security standards. As outlined below, we believe that, arguably, the information stored on the old HHT memory cards is not confidential information, and as such encryption is not required under DoITT's *Portable Data Security Policy.*

The auditor's response indicates that the old HHT memory card contains "application code, a database with a list of users assigned to the HHTs, their digital signatures, information regarding regulations, the names and addresses of repeat offenders, and data for all summonses that the HHT containing the memory card issued on that particular day." The HHT memory card does not contain application code. While digital signatures do exist on the cards, their use was discontinued. The remaining data on the memory card includes information regarding HHT users, regulations, repeat offenders, and summonses, all of which we believe to be public information.

Moreover, DoITT's *Portable Data Security Policy* was issued after DSNY deployed the old HHT devices. Rather than retrofit the old HHT devices, as noted, DSNY plans to discontinue the use of the old devices by May 2019, and has already begun to deploy newer HHT devices.

DSNY has taken steps to ensure that the new HHT devices meet all applicable security standards. The new HHTs are locked using Microsoft's [redacted] software, and employ two-factor authentication requiring both an encrypted pin code which exists on a database in the device, and an RFID enabled user identification card for login. All data required for device login is encrypted. As with the older devices, the newer HHT devices contain unencrypted information regarding HHT users, regulations, repeat offenders, and summonses, all of which we believe to be public information.

As an additional security feature, the new HHTs can only communicate with the DSNY network if plugged into a valid cradle in at the location to which the device is assigned. DSNY does not activate the generic "security features enabled" setting on the new HHT devices as we have confirmed with [redacted] that anti-virus software is not available for hand held devices. To access data stored on a device, a malicious actor would need both physical access to the HHT itself and the correlating "cradle" in order to overcome the device's security features.

## Lack of Protection for Transmitted and Stored Data

***Finding # 8***

***Two Critical Applications, and Two Non-Critical Applications, Used an Unsecured Network Protocol***

*According to DoITT's Encryption Policy, "All City of New York data with a classification of private or confidential may not be stored and/or transmitted across any communication mechanism unless it is protected using approved encryption technology." DoITT's Encryption Standard lists HTIPS as a supported, secure, alternative network protocol to the HTIP protocol for transmitting private or confidential information. Separately, DoITT's Application Security Policy states, "Protecting data's confidentiality, integrity, and availability is a principle that must be maintained at all times. Proper encryption solutions must be implemented to protect data at rest, in use or in motion." However, four DSNY applications do not protect data in motion.*

*During application walkthroughs of 10 critical and 10 non-critical applications, and system tests of six critical applications, we determined that DSNY implemented two critical and two non-critical web-based applications that use an unsecured communications protocol, HTIP, which does not comply with DoITT's policies and standard. Specifically, DSNY's critical applications* [redacted] *and its non-critical applications* [redacted] *use the unsecured HTIP protocol rather than the secure HTTPS protocol.*[14]

*The HTTPS encrypted protocol ensures that transmitted data and messages can be read by only the two parties involved in the conversation. An unsecured protocol does not provide that protection and potentially could allow the communication to be intercepted and read by an unauthorized individual. DSNY applications should use the secure HTTPS protocol. In our follow-up communications regarding this issue, as of February 15, 2019, DSNY stated that it had implemented the required change for the* [redacted] *applications. Further, according to DSNY, the* [redacted] *application will be replaced. However, DSNY did not provide a replacement date. Until the application is updated to the secure protocol, it poses the risk of having an unauthorized user gaining access and reading the data.*

***Recommendation # 8***

*DSNY should ensure all web-based applications utilize the secure HTTPS protocol.*

**Agency Response # 8**

As noted in the Auditor's report, we have remediated the [redacted] applications.

As noted in Agency Response to Finding #3 above, the [redacted] application interfaces with the [redacted] owned by the Department of Citywide Administrative Services (DCAS). Replacement of [redacted] requires coordination with DCAS, and a replacement date has not yet been agreed to.

***Finding # 9***

***One Application Failed to Protect DSNY's Scanned Documents with Encryption***

*As noted above, DoITT's Application Security Policy requires proper encryption solutions to protect data at rest, in use, or in motion. However, during the application walkthroughs of 10 critical and 10 non-critical applications, we found that DSNY's [redacted] application was noncompliant in that it stored and accessed approximately six million scanned documents that currently are not encrypted. The use and storage of unencrypted scanned documents could lead to the improper exposure, theft, modification, or deletion of the data they contain. In our discussion of this issue, DSNY explained that its [redacted] team plans to encrypt existing and future documents and that it expected the encryption project to start in March 2019 with a duration of 12 to 18 months, depending on resource availability. As of the date of this draft report DSNY has not started the encryption project to protect its scanned documents.*

***Recommendation # 9***

*DSNY should ensure all [redacted] scanned documents are protected with encryption.*

**Agency Response # 9**

Contrary to the audit finding, as of the date of the auditor's report DSNY had started the [redacted] encryption project. (In fact, the 12 to 18 month duration estimate itself evidences discussions and a project plan). To date, the [redacted] application has been moved to the cloud, and we are actively working to upgrade the application, both of which are prerequisites to enabling encryption of existing and future documents stored in [redacted]. The 12 to 18 month estimate, with a start in March 2019, remains accurate.

## *Vulnerability Management Program Shows Deficiencies*

***Finding # 10***

***The Agency Has Not Conducted Application Vulnerability Scans on Three Critical Applications***

*DoITT's Vulnerability Management Policy states, in part, "All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." The policy further states that "[v]ulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation." To assess DSNY's vulnerability management program, we requested application vulnerability scans for all critical applications. However, the agency did not provide vulnerability scans for three critical applications, [redacted].*[15]

*Information security involves an ongoing process of finding and addressing security gaps, including by periodically performing vulnerability scans. Open vulnerabilities must be resolved rapidly to prevent attackers from exploiting them to access sensitive and confidential information and possibly degrading system operations and damaging data. In response to our finding DSNY tentatively scheduled vulnerability scans of the three abovementioned applications as follows: [redacted] vulnerability scans are in progress with target dates of February*

*1 and 15, 2019, respectively; a* [redacted] *vulnerability scan is scheduled for the week of May 6, 2019.*

***Recommendation # 10***

*DSNY should periodically conduct necessary vulnerability scans of critical applications, address any vulnerabilities found, and conduct a follow up scan to confirm vulnerability remediation, as directed in DoITT's Vulnerability Management Policy.*

**Agency Response # 10**

As a New York City agency, DSNY relies on DoITT and NYC3 to monitor for system vulnerabilities. We provided system scans at the auditor's request, however we rely on DoITT to maintain a vulnerability management program and process.

**Finding # 11**

***The Agency's Network Vulnerability Scan Reports Were Unreliable***

*NIST Special Publication 800-53 states, "Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations." The publication further explains that correlating the results of multiple monitoring tools helps an organization to build, operate, and maintain effective monitoring tools:*

> *The organization correlates information from monitoring tools employed throughout the information system. . . . Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs.*

*However, DSNY did not ensure that its network vulnerability tool operates correctly. As part of the audit, we asked DSNY to provide us with network scan reports. In response, the agency provided a network scan report from June 6, 2018, which revealed several vulnerabilities. We informed DSNY of the vulnerabilities identified in the report and later asked for a new network scan report to determine whether the initial vulnerabilities were addressed. DSNY thereafter provided us with two additional network scan reports dated July 13, and 24, 2018, respectively, which showed the same vulnerabilities as had been revealed by the June 6, 2018 report-vulnerabilities that the agency claimed it had addressed. DSNY officials stated that they have been working with DoITT to resolve these issues and informed us that the scan reports were unreliable. Unreliable vulnerability scan reports prevent the agency from knowing about the weaknesses in the network or confirming the success of efforts to remove the vulnerabilities. Such knowledge is essential to enable the agency to resolve weaknesses that could allow a malicious actor to gain access to computers and data and, for example, steal data, or initiate a ransomware attack that could disable the agency's computers and cut off its access to the data it needs to operate.*

*On December 28, 2018 DSNY informed that the issue with the network scan reports has been resolved and provided us with three new consecutive network scans that showed that the agency had addressed the previously-found vulnerabilities. However, the three new reports showed that several DSNY computers were using an outdated operating system, which pose new previously unidentified vulnerabilities and place the network infrastructure at risk. We asked DSNY about the new vulnerabilities and, as of February 15, 2019, the agency responded that it has removed the machines with the outdated operating system from its network. However, DSNY did not provide a follow up vulnerability scan report to confirm that the vulnerabilities were addressed.*

***Recommendation #11***

*DSNY should test all vulnerability scanning tools to assess the reliability of the scanning results, and correlate the results from vulnerability scanning tools with the output of other security tools, as recommended by the National Institute for Standards and Technology (NIST).*

**Agency Response # 11**

As a New York City agency, DSNY is mandated to use the network vulnerability tools and associated scan reports selected, owned, and maintained by DoITT and NYC3. As such, it is not possible for DSNY to ensure that the network vulnerability tool operates correctly, or that the scans are accurate. As noted, we can, and do, work with DoITT and NYC3 to resolve tool or report issues when we become aware of them. In some cases it may not be clear to DSNY that a tool output or scan report is not accurate or reliable.

Will request a vulnerability scan from DoITT and NYC3 to confirm that the risk posed by computers with outdated operating system no longer exists following the removal of the computers.

## Pending Risk Assessment Report Recommendations

**Finding # 12**

**Pending Risk Assessment Report Recommendations**

The auditor's report states, in relevant part:

> To determine its security posture, DSNY requested a security program assessment from a third-party vendor and obtained the vendor's report on July 1, 2016. . . . [the] security program assessment report made seven recommendations that had a two-year roadmap for implementation (July 1, 2016 to July 1, 2018), and included several observations relating to security areas. As of December 2018, DSNY had implemented two of these recommendations, had not implemented one, and had partially implemented the remaining four. In addition, DSNY had not addressed one finding mentioned in the observations section of the report.

Specifically, DSNY had not fully implemented the following five recommendations (one not implemented and four partially implemented): a security governance program; an assessment of current skills; a data classification program; an SDLC process to identify and remediate vulnerabilities in DSNY applications; and a security training and awareness program. And the agency had not addressed a separate observation in the report-the lack of a disaster recovery plan to address an agency-wide disruptive cyber event. After we discussed this finding with DSNY officials during the audit, the agency reported taking additional action; specifically, on February 15, 2019, DSNY informed us that the SDLC process has been integrated into the work of its project management office, and that DSNY is currently working with NYC3 to conduct vulnerability scans. The agency also stated that it is ready to conduct NYC3-provided security awareness training but is waiting for NYC3 to start the training campaign. DSNY further informed us that NYC3 has taken the lead on a citywide data classification project and will provide a citywide solution that DSNY will leverage to address the need. In addition, DSNY stated that it will take an additional two years to fully implement the remaining recommendations due to resource constraints.

***Recommendation # 12***

*DSNY should ensure that the recommendations made in the 2016 security assessment report are implemented.*

**Agency Response**

We address each of the security assessment items here. The actions referred to below were taken by DSNY prior to the start of the current audit.

**Implementation of**

1. **A security governance program; an assessment of current skills.**

   Security governance will be handled going forward in partnership with NYC3. As a result of the [redacted] assessment, DSNY hired a Chief Information Security Officer (CISO) and the DSNY CISO provided general security guidelines to the IT staff and trained the Desktop and Service Desk staff on how to deal with threats that we had identified. Revised security policies and procedures will be drafted by the DSNY CISO and/or NYC3. The network and server teams incorporate security guidelines and notify and work with the DSNY CISO on any new initiatives. The Project Management Office has incorporated security into the overall application development processes.

2. **A data classification program**

   As noted in the auditor's report, NYC3 has taken the lead on a City-wide data classification project and will provide a citywide solution that DSNY will leverage to address this need.

3. **A SDLC process to identify and remediate vulnerabilities in DSNY applications**

As noted in the auditor's report, a SDLC process has been integrated into the work of our project management office, and DSNY is currently working with NYC3 to conduct vulnerability scans.

4. **A security training and awareness program.**

   As noted in the auditor's report, DSNY is ready to conduct NYC3-provided security awareness training but is waiting for NYC3 to start the training campaign.

5. **A separate observation in the report-the lack of a disaster recovery plan to address an agency-wide disruptive cyber event.**

   DSNY, as well as other agencies, had believed that DoITT's disaster recovery site was built using virtualization technology such that the application environment on servers run from the site would function properly if and when needed. DoITT has recently provided clarity to DSNY that this is not the case. Instead, proper functioning of the DoITT recovery site requires that each application environment be rebuilt separately. We are in the process of rebuilding DSNY application environments for the DoITT disaster recovery site.