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 Department of Transportation's Access Controls over Its Computer Systems

SI17-107A
February 6, 2018
http://comptroller.nyc.gov

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

February 6, 2018

To the Residents of the City of New York:

My office has audited the New York City Department of Transportation's (DOT's) access control over its computer systems to determine whether DOT had adequate system security and access controls in place to protect information in its computerized environment. We conduct computer system audits such as this to help ensure the integrity of the data stored in those systems and to minimize the risk of improper access to the City's systems.

The audit determined that DOT has established controls for application access and data protection and that it has implemented security controls to protect its computerized environment. However, we found weaknesses in certain of those access and security controls. Specifically, we found that DOT had not deactivated or disabled the user accounts for former or on-leave employees and had not implemented and enforced the Department of Information Technology and Telecommunications' (DoITT's) password expiration and complexity rules for three critical applications. We also found that two DOT public web applications, Annual Overweight Load Permits (AOL) and Over-Dimensional Overweight Vehicle Permits (ODVP), used an unsecured network protocols. Further, we found that DOT had not classified its data into public, sensitive, private or confidential categories as prescribed by DoITT policy and had not promptly addressed reported vulnerabilities in several servers and that the agency was using a server configuration with an outdated, unsecured encryption protocol.

The audit makes 10 recommendations, including: that DOT immediately disable former and inactive employees' user accounts in all of its applications; that DOT ensure that the AOL and ODVP applications, and all web-based, public-accessed applications that handle private or confidential data, utilize the secure Hypertext Transfer Protocol Secure (HTTPS) protocol; and that DOT address all detected vulnerabilities by applying the proper patches and configuration changes.

The results of the audit have been discussed with DOT 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 Department of Transportation's Access Control over Its Computer Systems SI17-107A

EXECUTIVE SUMMARY

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

DOT manages one of the most complex urban transportation networks in the world. It is responsible for the condition and operation of 6,300 miles of streets, highways, public plazas and 789 bridge structures. It maintains over one million street signs, 12,700 signalized intersections, over 315,000 street lights, and over 200 million linear feet of markings. In addition, it manages and maintains the City's streets, sidewalks, curbside parking, bike lanes, bus lanes, and un-tolled bridges, as well as the Staten Island Ferry.

As part of its operations, DOT uses 88 computer applications. The agency identified 15 of those applications as critical. The 15 critical applications process private information in addition to public data. The private information includes driver's license numbers, personal medical data, the names and addresses of the employers of permit applicants, and other information restricted to agency use. All of DOT's applications and their data are regulated by the agency's policies and the New York City Department of Information Technology and Telecommunications' (DoITT's) policies.

Audit Findings and Conclusions

Our audit found that DOT has established controls for application access and data protection, and has implemented security controls to protect its computerized environment. However, we found weaknesses in certain of those access and security controls. Specifically, DOT had not deactivated or disabled the user accounts of 113 former or on-leave employees, as required by DoITT's policies, increasing the risk that unauthorized users could gain access to DOT's applications and attempt to modify, delete, or steal data. In addition, DOT did not implement and enforce DoITT's password-expiration and complexity rules for three critical applications. We also found that two DOT public web applications, Annual Overweight Load Permits (AOL) and Over-Dimensional Overweight Vehicle Permits (ODVP), used an unsecured network protocol—a method by which computers communicate with each other—that rendered the applications and the communications the protocol carries vulnerable to unauthorized intrusion and interception.

Further, as of September 14, 2017, DOT had not classified the data in the majority of its applications into public, sensitive, private or confidential categories as prescribed by DoITT policy. Data classification is a critical step toward determining whether security controls are adequate for different sets of data. DOT has also initiated but not completed a comprehensive risk assessment of its computer systems, which is necessary to identify and address system and data security requirements. The audit also found that DOT had not promptly addressed reported vulnerabilities in several servers and that the agency was using a server configuration with an outdated, unsecured encryption protocol.

During the audit and the exit conference on December 6, 2017, DOT 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 above-mentioned issues, we made the following 10 recommendations to DOT:

- Immediately disable former and inactive employees' user accounts in all of its applications and thereafter conduct periodic reviews to identify and disable the application user accounts of former and inactive employees.
- Ensure that DOT's Human Resources Department promptly informs the Information Technology Administrators in charge of maintaining user accounts when an employee leaves the agency or goes on long-term leave.
- Ensure all current and future applications follow DoITT's security policies and allow for the deactivation of former or on-leave employees without loss of data the agency needs to retain.
- Review the system controls and procedures in place and modify them if necessary to ensure that user accounts are promptly deactivated for people who are separated from DOT.
- Ensure all applications follow DoITT's Identity Management and Password Policies.
- Ensure that the AOL and ODVP applications, and all web-based, public-accessed applications that handle private or confidential data utilize the secure Hypertext Transfer Protocol Secure (HTTPS) protocol.
- Ensure that agency-wide data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.
- Implement the necessary controls to prevent, detect and block the theft of data via external devices connected to its computers such as USB storage drives and portable hard drives.
- Address all detected vulnerabilities by applying the proper patches and configuration changes; a follow-up network vulnerability scan report should also be generated to confirm that mitigation of vulnerabilities has taken place.
- Complete a risk assessment of its systems and data as described in National Institute of Standards and Technology's (NIST's) Cybersecurity Framework and in the Center for Internet Security's (CIS's) Critical Security Controls.

Agency Response

In its response, DOT agreed with all 10 of our recommendations. However, DOT took issue with one finding, stating that "[t]he report does not accurately present the correct number of employees who had unauthorized access to critical applications. The report cites 113 employees who had unauthorized access and the accurate figure is 52."

AUDIT REPORT

Background

DOT oversees one of the most complex urban transportation networks in the world. It is responsible for the condition and operation of 6,300 miles of streets, highways, public plazas and 789 bridge structures. It maintains over one million street signs, 12,700 signalized intersections, over 315,000 street lights, and over 200 million linear feet of markings. Moreover, it manages and maintains the City's streets, sidewalks, curbside parking, bike lanes, bus lanes, and un-tolled bridges, as well as the Staten Island Ferry.

DOT's major services are to: 1) maintain the transportation infrastructure; 2) provide a safe transportation network; 3) design and build transportation alternatives by increasing ferry services, installing bike racks, increasing bike lane miles, and increasing Select Bus Service routes; 4) design public space to facilitate livability; and 5) deliver projects on time. DOT's Information Technology and Telecommunications unit (IT&T) provides technological infrastructure and support for the agency's services and operations.

As part of its operations, DOT uses 88 computer applications.[1] The agency identified 15 of these 88 applications as critical based on the following criteria: the system is directly aligned with the agency's core mission; it has a large number of users; and its unavailability would cause a severe hardship to DOT's operations. Among DOT's critical applications are the Dynamic Access System for Highway Inspection and Quality Assurance (DASH), the Emergency Snow Report, and the ePermits and the Bridge Data System (BDS) applications. The DASH application helps field inspectors address citizen complaints about street and highway construction work. The Emergency Snow Report application surveys various DOT units and generates a report during severe snow events that is shared with New York City Emergency Management and other agencies. The ePermits application provides the public, government agencies, and not-for-profit organizations a means to apply for parking permits. Lastly, the BDS application tracks DOT's inspection of NYC-managed bridges.

The agency's 15 critical applications contain private information in addition to public data. The private information that is collected, processed, transmitted or stored by these applications can include driver's license numbers, personal medical data, employer names and addresses, and information restricted to agency use. All of DOT's applications and their data are regulated by the agency's policies and DoITT's policies.[2] Table I below shows some of DoITT's pertinent policies applicable to DOT's systems.

[1] The agency provided a list of 89 applications in use on June 8, 2017. One application, the Voucher Payment System, was taken off the list on July 10, 2017, bringing the total number of applications in use at the agency to 88.

[2] DoITT states that it provides for the sustained, efficient, and effective delivery of IT services, infrastructure, and telecommunications to enhance service delivery to the City's residents, businesses, employees, and visitors. DoITT serves a vast network of 120 City agencies, boards, and offices, more than 8,000,000 city residents and 300,000 employees every day.

Table I

DoITT Policies

Policy Name	Policy Text Excerpts
Citywide Application Security Policy	"All applications must implement adequate security measures to protect the confidentiality, integrity and availability of data at rest, in use or in motion."
Citywide Data Classification Policy	"The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation."
Citywide Encryption Policy	"All City of New York data with a data classification of private or confidential may not be stored and/or transmitted across any communication mechanism unless it is protected using approved data encryption technology."
Citywide Password Policy	"Passwords and PINS must have a minimum length of eight (8) characters. . . . Passwords must contain at least one alphabetic character and at least one numeric or special character. . . . Passwords must expire at least every 90 days."
Citywide Identity Management Security Policy	"Each agency is responsible for the management of its user identities. This includes identity validation/ registration, authentication, authorization, provisioning /de-provisioning and management of identities. … User accounts will be created and de-provisioned in a timely manner."[3]

To accomplish the mandated level of security, DOT must establish and maintain appropriate access controls, including user authorization, identification, authentication, access approval and login credentials. DOT also has the responsibility to ensure that it implements and maintains controls to protect information in the agency's computerized environment, in compliance with the agency's and DoITT's policies.

Objectives

The objective of this audit was to determine whether DOT had adequate system security and access controls in place to protect information in its computerized environment.

[3] We use the terms disable, remove, delete, deactivate, and de-provision interchangeably, as they appear in various City policies that concern the management of user accounts in City computer systems.

Scope and Methodology Statement

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

The scope of this audit was from February 27, 2017 through September 14, 2017. We conducted fieldwork from March 13, 2017 through September 14, 2017. 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 DOT officials during and at the conclusion of this audit. A preliminary draft report was sent to DOT and was discussed at an exit conference on December 6, 2017. On January 2, 2018, we submitted a draft report to DOT with a request for comments. We received a written response on January 17, 2018. In its response, DOT agreed with all of the 10 recommendations. However, the agency stated that "[t]he report does not accurately present the correct number of employees who had unauthorized access to critical applications. The report cites 113 employees who had unauthorized access and the accurate figure is 52."

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

FINDINGS AND RECOMMENDATIONS

The audit found that DOT has established controls for application access and data protection, and has implemented security controls to protect its computerized environment.[4] However, we found weaknesses in certain of those access and security controls. Specifically, DOT had not deactivated or disabled the user accounts of 113 former or on-leave employees, as required by DoITT's policies, increasing the risk that unauthorized users could gain application access and attempt to modify, delete, or steal data. In addition, DOT did not implement and enforce DoITT's password expiration and complexity rules for three critical applications. We also found that two DOT public web applications, AOL and ODVP used an unsecured network protocol—a method by which computers communicate with each other—that rendered the applications vulnerable to eavesdropping by anyone able to intercept the communications the protocol carries.[5]

Further, DOT has not classified its data into public, sensitive, private or confidential categories as prescribed by DoITT's policy. Data classification is a critical step towards determining whether security controls are adequate for different sets of data. DOT has also not completed a risk assessment of its computer systems, which is necessary to identify and address system and data security requirements.[6] The audit also found that DOT had not promptly addressed reported vulnerabilities in several servers and that the agency was using a server configuration with an outdated, unsecured encryption protocol. The above-mentioned vulnerabilities, if not addressed, present an increased risk that unauthorized individuals could gain access to restricted information, modify, delete and steal data, and shut down the server and affect services.[7] Open vulnerabilities must be resolved rapidly to prevent attackers from accessing sensitive and confidential information and damaging system operations and data.[8]

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

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

Unauthorized Access to Critical Applications–113 Former and On-leave Employees Still Had Computer Application Access

DOT is responsible for creating and monitoring access to its applications for its authorized users and for disabling their access when their employment status changes. However, the agency did

[4] DOT's computer infrastructure is covered, in addition to its own controls, by DoITT's security controls such as antivirus, antimalware, and other IT security services.
[5] DoITT's Encryption Standard defines network security protocols as a type of network protocol that ensures the security and integrity of data in transit over a network connection. The Encryption standard lists Hypertext Transfer Protocol (HTTP) as an unsecure network protocol and presents HTTP Secure (HTTPS) as a secure alternative.
[6] The risk needs to be assessed first before it can be responded to. The National Institute of Standards and Technology states that risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. NIST Special Publication 30 revision 1: Guide for Conducting Risk Assessments.
[7] NIST defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. NIST Special Publication 30 revision 1: Guide for Conducting Risk Assessments.
[8] Delay in addressing vulnerabilities has serious repercussions. It has been reported that in March 2017 the credit bureau Equifax experienced a massive data breach that compromised the data of 145.5 million people. The attackers reportedly used a vulnerability to access Equifax systems. Although a patch to correct the vulnerability had been available since March 2017, Equifax reportedly had not applied it two months later, as of mid-May 2017, when the attack occurred. *See* Cowley, Stacy, *2.5 Million More People Potentially Exposed in Equifax Breach,* New York Times, October 2, 2017.

not ensure that user accounts for 9 critical applications were promptly deactivated for 113 former or inactive employees who either had left agency service or had gone on long-term leave.[9]

DOT's Access Control Policy states, "All user IDs for inactive accounts over 90 days old must be either removed or disabled."[10] In addition, DoITT's Identity Management Security Policy states that user accounts will be created and de-provisioned in a timely manner. Comptroller's Directive #18 § 8.1.2 requires the "deactivation of inactive user accounts and accounts for employees whose services have been terminated."

We analyzed DOT's lists of active user accounts for nine critical applications as of August 4, 2017, and found that they included 153 active user accounts for individuals listed in the City's Payroll Management System (PMS) as former employees or employees on long-term leave. At the exit conference, DOT officials stated that some of the above-mentioned 153 users were consultants, expediters, or active employees. After reviewing the supporting documentation DOT provided, we found that 40 of the 153 user accounts in question were assigned to individuals based on their current status as employees, consultants or expediters. DOT did not provide supporting documentation for the remaining 113 active accounts of users found in PMS as former and on-leave employees.

Table II below shows the numbers of employees, by year, with active user accounts who had previously ended their agency employment status, according to the PMS database.

Table II

Number of Former and On-leave Employees Found in Active User Account Lists per Year as of August 4, 2017

Year(s) in Which Employees Became Separated from City Employment per PMS	Number of Former and On-leave Employees Included in DOT Active User Account Lists
2017	19
2016	17
2015	5
2014	6
2013	5
2000-2012	31
1984-1999	30
Total	**113**

DOT officials also stated at the exit conference, without providing verifiable supporting documentation, that 61 of the above-mentioned 113 user accounts had been deactivated in the agency's Active Directory, and therefore those users would not be able to access to the agency's

[9] Long-term leave includes child care leave and approved leave without pay due to illness.
[10] DOT's Access Control Policy defines user ID as follows: "Account (User ID or Username) – A unique string of characters assigned to a user by which a person is identified to a computer system or network."

applications, notwithstanding that their accounts continued to be listed as active in those applications.[11]

Separately, during our walk-throughs, DOT stated that inactive user accounts could not be deleted or deactivated because several applications linked data regarding agency transactions to those user accounts and that data would be lost if the user account was deleted.[12] DOT added that the agency created long and complex passwords for each inactive user account, to secure the account and protect the application and its data. But while the use of such passwords may provide a measure of protection, it does not afford the same level of security provided by disabling the user account and is not an acceptable substitute control under applicable City policies. DOT should instead upgrade its applications to enable it to retain all necessary data while timely deactivating user accounts.

Timely deactivation of user accounts is necessary for the security of sensitive data that exists in DOT's information systems. DOT's ePermit application, for example, provides the public and other government agencies a means to apply for parking permits. That system retains health-related data and driver's license data provided by applicants, which is confidential and should be restricted to authorized use. The continued existence of active user accounts assigned to individuals who have left DOT—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 important that DOT promptly deactivate the user accounts of individuals who are no longer authorized to access its applications.

DOT Response: "The report does not accurately present the correct number of employees who had unauthorized access to critical applications. The report cites 113 employees who had unauthorized access and the accurate figure is 52.

DOT submitted a comprehensive spreadsheet to the Comptroller's auditors at our exit conference which indicated that 61 of the 113 accounts had already been deactivated or were non-existent in DOT's Active Directory. The Comptroller's Office requested supporting documentation for this. However, as communicated to the auditors, DOT could not provide supporting documentation available from any IT generated report that can be issued directly from the system to confirm that the 61 accounts were in fact deactivated. It is for this reason we invited the Comptroller's auditors to conduct a physical observation of our system to confirm that these 61 employees were in fact no longer in active status.

In response, rather than accepting our invitation, the auditors requested screenshots of each of the 61 deactivated accounts. We provided the screenshots as requested. However, the next business day, the auditors stated that the screenshots were not sufficient evidence. When DOT again suggested that the auditors come to DOT to perform a physical observation of the Active Directory Management Console, which lists all active accounts, the auditors declined our invitation to perform such an observation.

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

[12] An inactive account is a user account that has not been used for a period of time.

It should be noted that physical observation is considered one of the best types of audit evidence because it is 'Direct Evidence' of something seen by the auditors themselves. Their unwillingness to schedule a meeting to review the deactivation status, is inconsistent with audit protocol and has resulted in an inaccurate conclusion/finding."

Auditor Comment: DOT was first provided with this audit's findings in August 2017, after which we made numerous requests for the agency to provide evidence that would refute any of these findings. Our audit findings specifically included that during the audit period, 113 active users were listed in PMS as former employees or employees on long-term leave. Although DOT had ample opportunity between August 30, 2017 and January 2, 2018, the date the draft report was issued, to provide sufficient evidence to confirm its claim that 61 of the 113 employees were no longer in active user status, DOT never did so. Rather, it was only *after* the draft audit was issued to DOT that it provided print screenshots for the 61 users, and those screenshots did not contain any evidence of when the users' access had actually been disabled, such as a date or timestamp in the screenshots. Without such evidence, we were unable to determine whether the 61 users had been disabled during our audit period or even any time before we informed DOT of our finding.

Moreover, following notice of our finding but prior to the issuance of the draft report, DOT never requested that the auditors observe the system as an alternative means of verifying the agency's claim that access for the 61 individuals had been deactivated in the system. While after the draft audit report had been issued and shortly before DOT's response was due, DOT requested such an observation of its system to verify that the 61 users had been disabled, that observation would not have, at that late date, provided reliable evidence that the 61 users had had their accounts deactivated *prior* to the draft audit being issued. Accordingly, although as a general rule "physical observation is considered one of the best types of audit evidence," this principal does not apply when the observation could not have confirmed that an observed condition had existed at an earlier point in time. Thus, DOT's claim that that only 52 users inappropriately remained in active user status and not 113 remained unsupported and we had no basis to credit it.

Finally, we note that in its response to this audit finding, DOT appears to minimize the significance of its having a system that allows any number of former employees and those on long-term leave to continue to have access to its computer systems. Whether the number is 52 or 113, DOT should recognize and address the serious risks of allowing any former or long-term leave employees access to critical applications.

Recommendations

DOT should:

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

   DOT Response: "DOT agrees with the auditors' recommendations for this finding and removed all of the former and inactive employees' accounts in all of its applications as well as in its Windows Active Directory.

   DOT is in the process on implementing automatic disabling of inactive accounts in our Active Directory. This should be completed this month. DOT will request its application developers to perform the same process in each of their applications as well with periodic reviews to confirm compliance."

2. Ensure that DOT's Human Resources Department promptly informs the Information Technology Administrators in charge of maintaining user accounts when an employee leaves the agency or goes on long-term leave.

   DOT Response: DOT agreed, stating, "To augment the monthly separation notification, DOT's Human Resources department now sends IT immediate notification of employee separations and future separations."

3. Ensure all current and future applications follow DoITT's security policies and allow for the deactivation of former or on-leave employees without loss of data the agency needs to retain.

   DOT Response: DOT agreed, stating, "IT discussed the recommended practice above with its application developers. This will be applied in all future applications and will be reviewed for feasibility in all current applications."

4. Review the system controls and procedures in place and modify them if necessary to ensure that user accounts are promptly deactivated for people who are separated from DOT.

   DOT Response: DOT agreed, stating, "We have begun implementing the above recommendation and will establish a written policy for future compliance."

Lack of Password Control in Three Applications

The establishment and enforcement of strong password policies are crucial tools enabling DOT to secure confidential data. However, the audit found that three of DOT's critical applications (BDS, Bidscope, and Speed Reducer Tracking System) do not comply with DoITT password complexity and expiration rules. DoITT's Password Policy states that "Passwords must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character . . . [and] Passwords and PINs must have a minimum length of eight (8) characters." The three above-mentioned applications accept passwords that did not meet those requirements. In addition, the applications did not comply with DoITT policy that passwords must expire at least every 90 days, or with Comptroller's Directive #18, §8.1.2, which requires that "users are forced to change passwords periodically." In fact, the three applications currently allow the use of passwords that never expire.

Auditors noted that the three applications in question were created more than 10 years ago, before compliance with DoITT's Password Policy was required. The BDS application was launched in 2006, the Bidscope application originated in 1998, and the Speed Reducer Tracking System (SRTS) application was rolled out in 2004. At this point, however, they should be brought into compliance with applicable Citywide security policies, including password control. At the exit conference, DOT officials stated that the three applications will be replaced in 2018 with applications compliant with applicable Citywide security policies.

Recommendation

DOT should:

5. Ensure all applications follow DoITT's Identity Management and Password Policies.

   DOT Response: "DOT agrees with the above recommendation. All three of the applications which lacked password controls were created prior to DoITT's Identity

Management and Password policies. These are legacy applications scheduled for replacement in mid-late 2018 (Speed Reducer and Bidscope) and Q3 of 2019 (BDS)."

Two Public Applications Use Unsecure Network Protocol

During an application walk-through, auditors determined that DOT implemented two web-based, public-accessed critical applications, AOL and ODVP that use an unsecure communications protocol, which does not comply with DoITT's Encryption Standard.[13] Specifically, DOT's AOL and ODVP critical applications use the Hypertext Transfer Protocol (HTTP) rather than the secure HTTPS 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 HTTP protocol for transmitting private or confidential information.

When data is transmitted over HTTPS encrypted protocol, it ensures that messages can be read by only the two parties to a communication. An unsecured protocol does not provide that protection. Since the public uses the applications to transmit personal information such as that contained in a driver's license, DOT's applications should use the secure HTTPS protocol. At the exit conference, DOT officials stated that HTTPS will replace HTTP in the two above-mentioned applications by January 2018.

Recommendation

DOT should:

6. Ensure that the AOL and ODVP applications, and all web-based, public-accessed applications that handle private or confidential data utilize the secure HTTPS protocol.

   DOT Response: "DOT agrees with the above recommendation. Both AOL and ODVP applications have been tested and functionally verified in our QA/Staging environment utilizing secure HTTPS protocol. They are scheduled to be moved to production before the end of January 2018."

Incomplete Data Classification and Data-Loss Prevention

Auditors found that, as of September 14, 2017, DOT had not classified the data in 85 of its 88 applications. At that time, only three of DOT's 88 applications complied with 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." By classifying the data and assessing its value to the agency, DOT can proceed to find adequate resources and means to protect it.

DoITT's policy requires that data be valued and categorized to:

[13] Computers communicate with other computers by following specific protocols. A protocol is a pre-established number of steps that computers must follow in order to communicate.

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection. 2) All information assets must be valued and categorized. 3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis. 4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Without the appropriate controls based on such classification, DOT data could be exposed to unauthorized access, modification, deletion or theft. Moreover, a number of DOT's applications collect, process, transmit or store the kind of information that under DoITT policy would be classified as private or confidential, such as driver's license numbers, personal medical data, employer names and addresses, and information restricted to agency use.

In addition, DOT does not have a system to detect and prevent the theft of the data it does classify as private or confidential via devices that can be attached to a computer, such as USB drives and external hard drives. DOT's Data Leakage Prevention Policy states, "No data categorized as PRIVATE or CONFIDENTIAL may be copied from the network to a portable data device (CD/DVD-ROM, USB drive, etc.) without authorization of the data owner." The Policy also states, "NYC Department of Transportation protects data against unwanted leakage and unauthorized use." While DOT has implemented three separate controls to detect and prevent data loss via email and via the internet, it has no controls in place to prevent and detect data theft via USB devices by internal and vendor staff with physical access to DOT's computers and servers.[14] In the absence of both a comprehensive data classification regimen and controls to prevent and detect unauthorized copying, the agency is vulnerable to the risk that its private and confidential data could be misappropriated.

At the exit conference, DOT officials stated that the agency was in the process of applying the above-cited DoITT data classification policy, and corresponding controls, to its applications; that the data in 95 percent of its applications had been classified as of December 5, 2017; and that all agency data will meet the classification policy, and steps will be taken to implement additional controls to protect it, by the end of 2018.

Recommendations

DOT should:

7. Ensure that agency-wide data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.

   DOT Response: "DOT agrees with the above recommendation. DOT has classified all of its production applications and has begun applying the information value and categorization as per DoITT's data classification policy. Some of the information is already protected at rest and in transit according to Citywide Encryption Standards. All of DOT's electronic information is highly available and recoverable as per DoITT's Data Classification Standard."

[14] The Data Loss Prevention controls DOT currently uses monitor email and internet usage.

8. Implement the necessary controls to prevent, detect and block the theft of data via external devices connected to its computers like USB storage drives and portable hard drives.

   DOT Response: "DOT agrees with the above recommendation. Aside from DOT's Access Control Lists and role based access, DOT is currently researching quality DLP (Data Loss/Leakage Prevention) solutions that will assist us in preventing, detecting and blocking the theft of data via external devices. DOT is also evaluating the feasibility of locking down USB ports for use only with DOT approved devices."

Servers Are Operating with Vulnerabilities

According to DOT's network vulnerability reports, the agency had several servers operating with unresolved vulnerabilities for eight months.[15] During the audit, the agency stated that it was aware of the vulnerabilities and that the vulnerabilities would be resolved by a software server upgrade. Server vulnerabilities allow attackers to gain access to execute commands on the servers that could enable them to gain unauthorized access to restricted information, modify, delete and steal data, and shut down the server and affect services.

DoITT's Vulnerability Management Policy, states, "All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." The policy further states that "[v]ulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the Citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation." Information security is an ongoing process of assessing and addressing security gaps. Network vulnerability scans, penetration testing, and network security assessments are procedures to measure the security posture of an entity's information technology systems and data. Once identified, security vulnerabilities need to be rapidly addressed.

DOT's network vulnerability report from February 24, 2017 disclosed 18 medium-level vulnerabilities within five of DOT servers. At the exit conference, DOT officials stated that all vulnerabilities had been remediated in their QA/Staging environment, and were scheduled for remediation in production pending Change Management approval.

Recommendation

DOT should:

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

   DOT Response: "DOT agrees with the above recommendation and we are actively addressing these matters. DOT has remediated the vulnerabilities found on its public facing servers in our QA environment. The final vulnerability is scheduled for remediation in our production environment on Thursday, January 18, 2018. DoITT performs scheduled vulnerability scans via its MVM (McAfee

[15] One report was generated by DOT on February 24, 2017. A second report showing the same unresolved vulnerabilities was generated on September 7, 2017.

Vulnerability Manager) every weekend. DOT will be reviewing the report every week and address any new vulnerabilities found."

Risk Assessment of Information Technology Systems Is Not Comprehensive

DOT has not completed a risk assessment of its information systems and data, as advocated by NIST for critical infrastructure organizations such as DOT. In the absence of a completed risk assessment, DOT cannot address all potential risks to its computer systems.

DOT provided an initial risk assessment profile of its systems based on NIST's Cybersecurity Framework.[16] However, the Cybersecurity Framework details a five-phase process where an initial risk profile is created in phase one. A target risk profile should then be created in phase two. The initial profile is the "as is" state, and the target profile is the "to be" state. The third phase comprises the various tasks conducted to move the entity from its initial profile state to the target profile state. Phase four assesses the progress toward the target state, and phase five establishes communication among internal and external stakeholders about cybersecurity risk.

In response to our inquiry about the completion of DOT's risk assessment, DOT officials stated on September 12, 2017 that

> based on the current risk assessment, we will identify those items on the NIST Cybersecurity Framework where we scored low and are also of considerable risk to the Agency. We will use this criteria to place the risks in order of importance and begin addressing them in that order. We also plan to begin implementing the Center for Internet Security's (CIS's) Critical Security Controls (CSC) for effective cyber defense. Once we've had a chance to review the current assessment we can create a target profile with realistic goals and achievable milestones.[17]

At the exit conference, agency officials stated that DOT completed current and target risk profiles using a CIS CSC risk assessment methodology. They also stated that DOT is creating an action plan to achieve the target state by the end of 2019, while concentrating on the first five Critical Security Controls in the first half of 2018.[18] DOT will continue its internal audit practice, and update its assessments and the action plan every six months.

[16] The Cybersecurity Framework is described in the NIST document Framework for Improving Critical Infrastructure Cybersecurity version 1.0, published on 2/12/14. The Cybersecurity Framework defines a framework profile as: "[It] represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario." The Framework has three components: the Framework Core; the Implementation Tiers; and the Profiles.

[17] CIS is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. www.cisecurity.org.

[18] CIS has developed a set of 20 Critical Security Controls that it recommends as a "must-do, do-first" starting point for organizations seeking to improve their cyber defense. https://www.cisecurity.org/controls/cis-controls-faq/ The first five CIS Critical Security Controls, version 6.0, are: (1) Inventory of Authorized and Unauthorized Devices; (2) Inventory of Authorized and Unauthorized Software; (3) Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; (4) Continuous Vulnerability Assessment and Remediation; and (5) Controlled Use of Administrative Privileges.

Recommendation

DOT should:

10. Complete a risk assessment of its systems and data as described in NIST's Cybersecurity Framework and CIS's Critical Security Controls.

    DOT Response: DOT agreed, stating, "DOT has completed phase one through three of our risk assessments based on CIS Critical Security Controls, and has begun phase four. Phase five (establishing communication among internal and external stakeholders about cybersecurity risk) is also in progress."

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 February 27, 2017 through September 14, 2017. We conducted fieldwork from March 13, 2017 to September 14, 2017.

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

- Reviewed DoITT's security policies and standards to determine current security policies in place that apply to City agencies.
- Reviewed DOT's 2015 response to Comptroller's Directive #1, to determine DOT's information technology status and application environment.
- Reviewed DOT's 2016 Strategic Plan and the Fiscal Year 2017 Mayor's Management Report to determine the agency's current goals, objectives, and priorities.

During the field work phase we:

- Requested and reviewed organization charts for the agency overall and the agency units responsible for DOT's information security to determine the organizational unit in charge of information security.
- Conducted walk-throughs of all DOT's critical applications to determine the security controls in place to safeguard the applications and data.
- Requested and reviewed policies, procedures, standards, strategic plans, best practices guides and change management controls for DOT's information security to determine the security controls implemented to protect information systems and data. Documents may originate from the agency or DoITT since it provides information technology services to the agency that include network infrastructure and security. Best practices and guides may be published by software and hardware vendors and computer security organizations, as well as by the agency.
- Requested and reviewed DOT'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 DOT'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 DOT's last information security audit, assessments reports, and results to determine information security controls implementation and performance.

- Requested and reviewed a list of DOT's critical software applications and systems to determine whether the critical applications have controls in place to safeguard the system and data.
- Requested and reviewed DOT's specific controls in place to prevent unauthorized access to critical applications and systems to determine the adequacy of the controls.
- Requested and reviewed DOT's detailed information security devices, applications, and services for the following security processes to determine the presence and maturity of specific information security controls: patch management, malware management, threat management, asset management, virus management, advanced persistent threat management, privileged user management, data loss/leak/exfiltration/corruption management, mobile device management, wireless access management, network access management, Bring Your Own Device (BYOD) management, backup/restore data management, access control management, incident response management, password management, awareness and training management, physical security management.
- Requested and reviewed DOT'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 DOT's latest security systems/devices logs, reports to determine the presence, and functionality of implemented information security controls.
- Requested and reviewed DOT's last reports of security incidents, system breaches, or cyber-attacks detected by, or reported to the information security team, as well as, measures taken to identify, isolate, mitigate, resolve or otherwise address the incidents.
- Requested and reviewed DOT'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 DOT's last incident response exercise report to determine effectiveness and maturity of incident response controls.
- Requested and reviewed DOT's last business continuity/disaster recovery exercise report to determine the effectiveness and maturity of such controls.
- Requested and reviewed DOT's last data backup/restore exercise report to determine effectiveness and maturity of security controls.
- Requested and reviewed list of all DOT's applications, critical and non-critical, hosted at DOT or by third parties, in production at DOT to determine the security controls in place to protect the systems and data.

During the fieldwork testing phase we:

- Requested and analyzed user lists for all DOT's critical applications to determine whether user lists of active staff contain inactive staff that should not have access to the applications. We also tested provided user account lists against City payroll database data.

- Requested read-only access for some of DOT's critical and non-critical applications to determine whether the applications follow password and other security policies. We tested compliance to DOT's and DoITT's applicable security policies.
- Conducted access control tests such as password format, length and complexity. Performed tests to determine whether DOT disables users after five sequential invalid login attempts within a 120-minute period, and has lock-out feature for after 15 minutes of inactivity.
- Requested and reviewed DOT's application vulnerability AppScan[19] reports for all critical applications to determine the security posture of each application. We requested follow-up application vulnerability reports to determine whether previously detected vulnerabilities have been addressed.
- Requested and reviewed DOT's network vulnerability report[20] to determine the network security posture. We requested a follow-up network vulnerability report to determine whether previously detected vulnerabilities have been addressed.

[19] The IBM Security AppScan 9.0.3.6 User Guide describes the AppScan application as a security vulnerability testing tool for web applications and web services. It features the most advanced testing methods to help protect your site from the threat of cyber-attack, together with a full range of application data output options.
[20] The network vulnerability report was generated by McAfee Vulnerability Manager on February 24, 2017 and provided by DOT. A second report dated September 7, 2017 showed that the vulnerabilities previously detected were not resolved.

NEW YORK CITY DOT Department of Transportation

POLLY TROTTENBERG, Commissioner

January 17, 2018

Ms. Marjorie Landa
Deputy Comptroller for Audit
The City of New York
Office of the Comptroller
1 Centre Street
New York, NY 10007

Re: NYC DOT's Response to Auditor's Draft Report on the Department of Transportation's Access Controls Over its Computer Systems (SI17-107A)

Dear Ms. Landa:

Thank you for providing the New York City Department of Transportation (DOT) an opportunity to respond to your office's draft report on the Department of Transportation's Access Controls Over its Computer Systems dated January 2nd, 2018. Please consider our attached comments **(See Attachment I)** prior to report issuance. Please extend our thanks to your staff for their work on this assignment.

Sincerely,

Amy Hutner
Auditor General

NYC Department of Transportation
Office of the Auditor General
55 Water Street, New York, NY 10041
T: 212.839.4408 F: 212.839.4926
Nyc.gov/dot

NEW YORK CITY DOT Department of Transportation
POLLY TROTTENBERG, Commissioner

Attachment I

NYC DOT's Response to Auditor's Draft Report on the Department of Transportation's Access Controls Over its Computer Systems (SI17-107A)

1) Unauthorized Access to Critical Applications – 113 Former and On-leave Employees Still Had Computer Application Access

Comment: The report does not accurately present the correct number of employees who had unauthorized access to critical applications. The report cites 113 employees who had unauthorized access and the accurate figure is 52.

DOT submitted a comprehensive spreadsheet to the Comptroller's auditors at our exit conference which indicated that 61 of the 113 accounts had already been deactivated or were non-existent in DOT's Active Directory. The Comptroller's Office requested supporting documentation for this. However, as communicated to the auditors, DOT could not provide supporting documentation available from any IT generated report that can be issued directly from the system to confirm that the 61 accounts were in fact deactivated. It is for this reason we invited the Comptroller's auditors to conduct a physical observation of our system to confirm that these 61 employees were in fact no longer in active status.
In response, rather than accepting our invitation, the auditors requested screenshots of each of the 61 deactivated accounts. We provided the screenshots as requested. However, the next business day, the auditors stated that the screenshots were not sufficient evidence. When DOT again suggested that the auditors come to DOT to perform a physical observation of the Active Directory Management Console, which lists all active accounts, the auditors declined our invitation to perform such an observation.

It should be noted that physical observation is considered one of the best types of audit evidence because it is "Direct Evidence" of something seen by the auditors themselves. Their unwillingness to schedule a meeting to review the deactivation status, is inconsistent with audit protocol and has resulted in an inaccurate conclusion/finding.

Response to auditors' recommendations:

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

   DOT agrees with the auditors' recommendations for this finding and removed all of the former and inactive employees' accounts in all of its applications as well as in its Windows Active Directory.

NYC Department of Transportation
Office of the Auditor General
55 Water Street, New York, NY 10041
T: 212.839.4408 F: 212.839.4926
Nyc.gov/dot

DOT is in the process on implementing automatic disabling of inactive accounts in our Active Directory. This should be completed this month. DOT will request its application developers to perform the same process in each of their applications as well with periodic reviews to confirm compliance.

2. **Ensure that DOT's Human Resources Department promptly informs the Information Technology Administrators in charge of maintaining user accounts when an employee leaves the agency or goes on long term leave.**

   To augment the monthly separation notification, DOT's Human Resources department now sends IT immediate notification of employee separations and future separations.

3. **Ensure all current and future applications follow DoITT's security policies and allow for the deactivation of former or on-leave employees without loss of data the agency needs to retain.**

   IT discussed the recommended practice above with its application developers. This will be applied in all future applications and will be reviewed for feasibility in all current applications.

4. **Review the system controls and procedure and modify them if necessary to ensure that user accounts are promptly deactivated for people who are separated from DOT.**

   We have begun implementing the above recommendation and will establish a written policy for future compliance.

2) Lack of Password Controls in Three Applications

Comment: As stated in the draft report, these applications are scheduled for replacement and will follow Identity Management & Password best practices.
Response to auditors' recommendations:

1. **Ensure all applications follow DoITT's Identity Management and Password Policies.**

   DOT agrees with the above recommendation. All three of the applications which lacked password controls were created prior to DoITT's Identity Management and Password policies. These are legacy applications scheduled for replacement in mid-late 2018 (Speed Reducer and Bidscope) and Q3 of 2019 (BDS).

3) Two Public Applications Use Unsecure Network Protocols

Comment: As stated in in the draft report both applications will begin using Secure Network Protocol this month (January, 2018).
Response to auditors' recommendations:

1. **Ensure that the AOL and ODVP applications, and all web-based, public-accessed applications that handle private or confidential data utilize the secure HTTPS protocol.**

   DOT agrees with the above recommendation. Both AOL and ODVP applications have been tested and functionally verified in our QA/Staging environment utilizing secure

NYC Department of Transportation
Office of the Auditor General
55 Water Street, New York, NY 10041
T: 212.839.4408 F: 212.839.4926
Nyc.gov/dot

HTTPS protocol. They are scheduled to be moved to production before the end of January 2018.

4) Incomplete Data Classification and Data-Loss Prevention

Comment: DOT will implement DoITT's Data Classification policy and corresponding controls by the end of 2018.
Response to auditors' recommendations:

1. **Ensure that agency-wide data classification is completed and appropriate controls are implemented to safeguard the data based on its classification.**

   DOT agrees with the above recommendation. DOT has classified all of its production applications and has begun applying the information value and categorization as per DoITT's data classification policy. Some of the information is already protected at rest and in transit according to Citywide Encryption Standards. All of DOT's electronic information is highly available and recoverable as per DoITT's Data Classification Standard.

2. **Implement the necessary controls to prevent, detect and block the theft of data via external devices connected to it computers like USB storage drives and portable hard drives.**

   DOT agrees with the above recommendation. Aside from DOT's Access Control Lists and role based access, DOT is currently researching quality DLP (Data Loss/Leakage Prevention) solutions that will assist us in preventing, detecting and blocking the theft of data via external devices. DOT is also evaluating the feasibility of locking down USB ports for use only with DOT approved devices.

5) Servers are Operating with Vulnerabilities

Comment: All vulnerabilities have been remediated in QA and will be moved to production in January 2018.

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

   DOT agrees with the above recommendation and we are actively addressing these matters. DOT has remediated the vulnerabilities found on its public facing servers in our QA environment. The final vulnerability is scheduled for remediation in our production environment on Thursday, January 18, 2018. DoITT performs scheduled vulnerability scans via its MVM (McAfee Vulnerability Manager) every weekend. DOT will be reviewing the report every week and address any new vulnerabilities found.

NYC Department of Transportation
Office of the Auditor General
55 Water Street, New York, NY 10041
T: 212.839.4408 F: 212.839.4926
Nyc.gov/dot

6) Risk Assessment of Information Technology Systems is Not Comprehensive

Comment: DOT will continue its risk assessment process utilizing the CIS CSC risk assessment methodology and updating its target profile every six months as stated in the draft report.

1. **Complete a risk assessment of its systems and data as described in NIST's Cybersecurity Framework and CIS's Critical Security Controls.**

   DOT has completed phases one through three of our risk assessments based on CIS Critical Security Controls, and has begun phase four. Phase five (establishing communication among internal and external stakeholders about cybersecurity risk) is also in progress. DOT now performs monthly phishing simulations and posting informational cybersecurity videos for our user community. We will be working with our Training Center to implement an Information Security Awareness program and mandatory training that will educate DOT employees about cybersecurity risks.

NYC Department of Transportation
Office of the Auditor General
55 Water Street, New York, NY 10041
T: 212.839.4408 F: 212.839.4926
Nyc.gov/dot