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 Development and Implementation of the NYCServ-Taxi Application Administered by the Office of Administrative Trials and Hearings

SI15-122A
June 16, 2016
http://comptroller.nyc.gov

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, NY 10007

SCOTT M. STRINGER
COMPTROLLER

June 16, 2016

To the Residents of the City of New York:

My office has audited the Office of Administrative Trials and Hearings' (OATH) NYCServ-Taxi application to determine whether it meets the overall goals as stated in the system specifications, has adequate functions to ensure the information process is reliable, and is secure from unauthorized access. We perform audits such as this to ensure that systems, technology development, and resources of City agencies are efficient, secure, and operate in the best interest of the public.

The audit determined that the overall goals of the NYCServ-Taxi application as stated in the system specifications have generally been met and have adequate functions and controls to ensure that the information processed is reliable. The audit also determined that the application is generally secure from unauthorized external access. However, our audit revealed that the NYCServ-Taxi application has internal security weaknesses. Specifically, Microsoft Windows password complexity is not enabled, web server security updates are not current, application access control vulnerabilities exist, and personally identifiable information (PII) is exposed.

The audit makes 10 recommendations that, if implemented, should mitigate the risks of the stated application security weaknesses and enhance access control. Specifically, OATH should coordinate with the Department of Information Technology and Telecommunication (DoITT) to enable password complexity, update and upgrade the application web server, remediate and restrict access to the application, and comply with PII classification policies as specified by DoITT.

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

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

Sincerely,

Scott M. Stringer

TABLE OF CONTENTS

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

Audit Report on the Development and Implementation of the NYCServ-Taxi Application Administered by the Office of Administrative Trials and Hearings

SI15-122A

EXECUTIVE SUMMARY

We audited the NYCServ-Taxi application administered by the Office of Administrative Trials and Hearings (OATH) to determine whether the application meets the overall goals as stated in the system specifications, has adequate functions to ensure the information process is reliable, and is secure from unauthorized access.

OATH is an administrative tribunal created by the City of New York (City) to independently adjudicate the disposition of certain City-issued civil violations and administrative claims. Its mission is to provide fair and unbiased administrative trials and hearings to New York City residents, businesses and City agencies. The OATH Hearings Division consists of the Environmental Control Board Tribunal (ECB), the OATH Taxi & Limousine Tribunal (TLT) and the OATH Health Tribunal. The OATH Taxi & Limousine Tribunal holds hearings on summonses issued by the New York City Taxi & Limousine Commission (TLC), the City's Police Department (NYPD) and the Port Authority of New York and New Jersey for alleged violations of TLC and other City rules.

In 2013, the OATH implemented a new $1.5 million electronic file and case management application called NYCServ-Taxi. Although the application is fully operational, further periodic enhancements are planned including an electronic interface with Taxi & Limousine Commission's computer environment.[1] Currently, adjudicated and reviewed results are manually entered into TLC systems by OATH's data entry personnel.

Audit Findings and Conclusion

Our audit found that the overall goals of the NYCServ-Taxi application as stated in the system specifications have generally been met. In addition, the audit found that the application has adequate functions and controls to ensure that the information processed is reliable. Further, the

[1] Enhancements include modifications to the application to accommodate periodic changes in the law, as well as the addition of new features and functions to the application.

audit found that the application, which is Intranet-based (that is, accessible through a web browser, but used primarily on the internal network of an organization), has restricted internal access, and has been generally secured from unauthorized external access.

However, the audit also found that the NYCServ-Taxi application has internal security weaknesses that require additional system modifications and controls to remediate risks. Specifically, the audit found the following areas of security weaknesses in NYCServ-Taxi application: Microsoft Windows password complexity has not been enabled; web server security updates are not current; there are application access control vulnerabilities, and Personally Identifiable Information (PII) is exposed.

Audit Recommendations

The audit made the following 10 recommendations:

- Coordinate with the Department of Information Technology and Telecommunication (DoITT) to enable password complexity in the Microsoft Window environment for protection of the computer system, and hosted applications.
- Test the updates to ensure their compatibility with the NYCServ-Taxi application, and apply the necessary security updates to the Web server in order to strengthen its security posture.
- Implement an enterprise patch management solution (i.e. Symantec, McAfee, Trend Microsystems) to ensure that the latest security patches and updates are applied.
- Take necessary steps to test future web server upgrades and then plan ahead to make necessary upgrades.
- Remediate the NYCServ-Taxi application to prevent unauthorized internal access by URL manipulation.
- Restrict access to NYCServ-Taxi webpages with administrator level functions designed for management to authorized users only.
- Ensure against similar deficiencies (web pages vulnerable to URL manipulation) in future application development projects by incorporating necessary steps into their Quality Assurance and Testing program.
- Comply with the DoITT Data Classification Policy to help guide its employees to alleviate the risk of collecting and storing PII into the NYCServ-Taxi application.
- Review the NYCServ-Taxi application data for PII and remove, block, or shield the information from unauthorized disclosure.
- Employ proper encryption methods to protect PII that is stored on the hard drives of computer systems or other network storage devices.

Agency Response

In its response, OATH generally agreed with the first three of four areas of audit findings and recommendations. OATH stated that it has taken appropriate action to alleviate and remediate the reported risks regarding internal security weaknesses. With regard to the findings and recommendations relating to Personally Identifiable Information (PII) exposure, OATH stated that it does not consider data collected by the NYCServ-Taxi application to be private data. In addition,

OATH stated that, to the degree it retains scanned images that require heightened security, it has adequate procedures in place to ensure these images are secure.

AUDIT REPORT

Background

The Office of Administrative Trials and Hearings is an administrative tribunal created by the City of New York to independently adjudicate the disposition of certain City-issued civil violations and administrative claims. Its mission is to provide fair and unbiased administrative trials and hearings to City residents, businesses and City agencies. OATH is organized into two divisions: the OATH Trials Division and the OATH Hearings Division. The OATH Trials Division adjudicates or settles a wide range of issues referred by City agencies. The OATH Hearings Division consists of the Environmental Control Board (ECB) Tribunal, the OATH Taxi & Limousine Tribunal (TLT), and the OATH Health Tribunal. It conducts hearings on alleged violations and summonses issued by various government agencies.

The TLT holds hearings on summonses issued by the New York City Taxi & Limousine Commission, the City's Police Department and the Port Authority of New York and New Jersey for alleged violations of TLC and other City rules. TLC-regulated vehicles include NYC medallion (yellow) taxicabs, for-hire vehicles (Boro Taxis, community-based liveries and black cars), commuter vans, para-transit vehicles (ambulettes) and certain luxury limousines.

In 2011, by Mayor's Executive Order 148, the tribunal functions of the TLC were transferred and consolidated into OATH. The tribunal was renamed the OATH Taxi & Limousine Tribunal, or TLT. Prior to the consolidation, and when the TLC still adjudicated the summonses, it relied on paper filings and a Microsoft Access database platform for case tracking.[2] In 2013, the TLT implemented a new $1.5 million electronic file and case management application called NYCServ-Taxi. The NYCServ-Taxi application incorporates features that meet the operational requirements of the TLT and four primary internal user groups: Customer Service, Data Entry, Hearing Examiner and Reviewer. The features of the new application include:

- Electronic archiving of case files;
- Recording and storage of audio hearing files;
- Digital scanning of evidentiary material presented at the hearings;
- Electronic transfer of summons information from the enforcement agencies;
- Automated mailing of TLT notices to parties involved in the hearings; and
- Case processing, management, and tracking.

The application, although fully operational, is expected to receive periodic enhancements. One such planned enhancement is an electronic interface with TLC's computer environment. This interface will enable case disposition results (e.g., guilty, not guilty, and hearing examiner findings) to be fed automatically into a TLC system. According to OATH officials, no date has yet been set for this electronic interface enhancement. Currently, adjudicated and reviewed results are manually entered into TLC systems by OATH's data entry personnel.

[2] Microsoft Access is a database management commercial off-the-shelf software package that generally runs on a Microsoft Windows operating system.

Objectives

The objectives of this audit was to determine whether NYCServ-Taxi:

1. meets the overall goals as stated in the system specifications;
2. has adequate functions to ensure the information process is reliable; and
3. is secure from unauthorized access.

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 in order to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the 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 focused on the NYCServ-Taxi application from its April 2012 inception through its operations in December 2015. We conducted audit fieldwork, which included testing from September 2015 through December 2015. Please refer to the Detailed Scope and Methodology at the end of this report for specific procedures and tests that we conducted.

Discussion of Audit Results

The matters covered in this report were discussed with OATH officials during and at the conclusion of this audit. A Preliminary Draft report was provided to OATH and discussed at an exit conference held on May 12, 2016. On May 24, 2016, we submitted a draft report to OATH with a request for comments. We received a written response from OATH on June 8, 2016. In their response, OATH officials generally agreed with the first three of four areas of audit findings and recommendations. OATH officials stated that the agency has taken appropriate actions to alleviate and remediate the risks regarding internal security weaknesses as stated in the audit report. Regarding the last area of audit findings and the related three recommendations pertaining to PII exposure, OATH stated that NYCServ-Taxi data and scanned images are generally not private. In addition, OATH stated that, to the degree it retains scanned images that require heightened security, it has adequate procedures in place to ensure these images are secure.

The full text of the OATH response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

The audit found that the overall goals of the NYCServ-Taxi application as stated in the system specifications have generally been met. In addition, the audit found that the application has adequate functions and controls to ensure that the information processed is reliable. Further, the audit found that the application, which is Intranet-based and has restricted internal access, has been generally secured from unauthorized external access .[3]

However, the audit also found that the NYCServ-Taxi application has internal security weaknesses that require additional system modifications and controls to remediate risks. Specifically, the audit found security weaknesses in the following four areas:

- Windows password complexity is not enabled: The Windows operating system used by NYCServ-Taxi does not enforce password complexity requirements, and thereby allows weak passwords;[4]
- Web server security updates are not current;[5] NYCServ-Taxi web server lacks periodic security updates, causing application vulnerabilities;
- There are application access control vulnerabilities: NYCServ-Taxi application webpage links are insufficiently protected against unauthorized internal access, resulting in:
    1. Possible unauthorized access to application webpages: We were able to access and retrieve summons information and user data from the application to access numerous webpages by manipulating the web address;
    2. URL manipulation granting inappropriate privilege-level access: NYCServ-Taxi application webpages for control and management of user access rights were not restricted only to administrator and management-level users;
- Personally Identifiable Information exposed: The names, addresses, email addresses and telephone numbers of the summons' respondents and their representatives are inadvertently stored in the application and open to general user access.

The above deficiencies stem from lapses in web server maintenance in the TLT computer environment, insufficient quality control and testing of the NYCServ-Taxi application prior to implementation in February 2013, and a lack of agency policy regarding data privacy. Additionally, password policy enforcement with regard to complexity has not been achieved. However, this is a system configuration issue that is outside of OATH's control.

Based on our concern over the immediate risk of an internal security bypass (inadvertent or intentional) into the NYCServ-Taxi application, we informed OATH of the security issues during the course of the audit. Prior to the close of audit field work, we were able to determine that OATH initiated remedial action towards protecting the NYCServ-Taxi application. However, as of the date of this report, we are not able to say if OATH's efforts have completely remediated the system weaknesses identified by the audit.

[3] An application developed using web internet technology making it accessible through web browsers such as Internet Explorer, and used primarily on the internal network of an organization.

[4] The Department of Information Technology and Telecommunication is responsible for setting the system's password complexity features and password policy enforcement.

[5] A Web server is a computer system that uses HTTP (Hypertext Transfer Protocol, the basic network protocol used to distribute information on the World Wide Web) to serve the files that form web pages for users.

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

Windows Password Complexity Is Not Enabled

We found that the TLT Microsoft Windows environment overall does not enforce password complexity as required by DoITT's *Password Policy*. We were able to change our network passwords and that change allowed us into the TLT Widows-based system several times using passwords which contain only numeric or only alphabetic values and thus have low security. While Windows checks for password length and history, it does not enforce strong password usage comprising of both alphabetic and numeric or special characters. Since the NYCServ-Taxi application also uses the same Microsoft Windows password to authenticate users' access into the application, we were able to access the application itself using the same weak password.

DoITT's *Password Policy* requires passwords to "be constructed using at least one alphabetic character and at least one character which is either numeric or special character." It further directs that passwords must not be derived from easily guessed, common words or phrases, nor should they be constructed from user IDs, proper names or other names, words, numbers or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or zip code).

OATH stated that DoITT established and maintained OATH's Microsoft Windows account and its password management services. As a result, OATH officials stated that the agency does not have the authority to make any changes to the operating system environment, and that such changes can only be made by DoITT.

Having a strong password is crucial for information security control. Weak passwords may be vulnerable to attacks, where a malicious user can run password generator programs against established user accounts until finding the correct password. A malicious user who gains access to these accounts can compromise an entire organization's network, installed applications and data because the same credentials are being used to access both.

Recommendation

OATH should:

1. Coordinate with DoITT to enable password complexity in the Microsoft Windows environment for protection of the computer system, and hosted applications.

OATH Response: "DoITT's security team is aware of this discrepancy and [OATH] will work with them to enable the complexity check, if possible."

Web Server Security Updates Are Not Current

The Web server that hosts the NYCServ-Taxi application is vulnerable to internal tampering due to missing security patches and software updates. According to the product's Software Security Team, these patches and updates are meant to fix "important" security vulnerabilities such as

DOS,[6] information disclosure,[7] HTTP request smuggling[8] and Security Manager Bypass.[9] As of the close of audit fieldwork in December 2015, the application was running on a webserver version originally released in 2013. In addition, the server version information was exposed on HTTP response code webpages we accessed during audit testing.[10] Server version information can help assist in malicious computer system attacks.

DoITT's *Vulnerability Management Policy* states that all computing resources directly and operationally controlled by the City of New York must be monitored for vulnerabilities and threats and must have action plans to remediate or mitigate vulnerabilities.

OATH is responsible for maintaining the Web server software, including installing periodic updates to the software in order to ensure a secure computing environment. This requires a plan for scheduling the necessary server updates to avoid interruptions to agency operations, and a process to test each update for compatibility prior to its release. However, OATH does not have such a plan and has not installed necessary software updates to alleviate system vulnerabilities, and nor does it have a plan to implement necessary software updates in the future. OATH officials stated that the agency has implemented an update to the web server in the past which caused a malfunction in the NYCServ-Taxi application.

Based on our observations and discussions during the course of the audit, OATH partially alleviated one of the vulnerabilities we identified by suppressing server identity information from HTTP error response code webpages.[11] However, the web server remained unpatched and outdated, leaving the TLT business operation vulnerable to internal tampering.

Recommendations

OATH should:

2. Test the updates to ensure their compatibility with the NYCServ-Taxi application, and apply the necessary security updates to the Web server in order to strengthen its security posture.

OATH Response: "There have been numerous compatibility issues between the application code and the later version of the web server software. As a result, and because of competing priorities, this upgrade has been a long-term project, which is ongoing. OATH will upgrade to the latest web server version as soon as possible. OATH can also agree to a more pro-active maintenance practice for web server updates once the upgrade to the current version is complete."

[6] A Denial-of-Service (DOS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

[7] Information disclosure is a type of attack aimed at acquiring system specific information about a website, including software distribution, version numbers and patch levels.

[8] HTTP Request Smuggling consists of sending a specially formatted HTTP request that will be parsed in a different way by the proxy system and by the final system, so the attacker could smuggle a request to one system without the other being aware of it.

[9] Security Manager Bypass is a technique used to bypass Web browser and computer operating system security restrictions.

[10] HTTP Response Codes indicate whether a specific HTTP request has been successfully completed.

[11] Server identity information includes software configuration and version details useful to a malicious user in computer attacks.

Auditor Comment: Although the agency plans to upgrade the web server software in the future, the recommendation as written was not addressed. The recommendation refers to the lack of security updates required to address current system vulnerabilities. Even if it upgrades the web server software, OATH will still need to address the issue of installing periodic security updates. Ignoring current threat exposure in lieu of a future upgrade with no timeline attached is against sound business practices. Unless it remediates the risks caused by outdated security updates, OATH assumes the risk that its web server's operating environment remains vulnerable to current and future exploits.

3. Implement an enterprise patch management solution (i.e. Symantec, McAfee, Trend Microsystems) to ensure that the latest security patches and updates are applied.

OATH Response: "OATH will upgrade to the latest webserver version as soon as possible. OATH can also agree to a more pro-active maintenance practice for web server updates once the upgrade to the current version is complete."

4. Take necessary steps to test future web server upgrades and then plan ahead to make necessary upgrades.

OATH Response: "OATH will upgrade to the latest webserver version as soon as possible. OATH can also agree to a more pro-active maintenance practice for web server updates once the upgrade to the current version is complete."

Access Control Vulnerabilities in NYCServ-Taxi Application

NYCServ-Taxi application webpages are insufficiently protected from unauthorized internal access. We replaced part of the web address with common words and some key words from NYCServ-Taxi User Manuals. By manipulating the web addresses, we were able to access various restricted webpages.

Unauthorized Access to Application Webpages

After logging into the application and manipulating the web address, we were able to use a read-only privilege level to gain access to numerous webpages that should have been restricted to users with higher privilege levels.[12] Furthermore, without logging into the NYCServ-Taxi application, we were able to access and retrieve summons and user data that should only be available to authorized and authenticated users.

URL Manipulation Grants Privilege Level Access

NYCServ-Taxi webpages for controlling the application and managing user access rights were not restricted to only administrator and management level users. By manipulating the web address as mention above, we were able to access administrator level functions such as granting, revoking and modifying user access rights in the NYCServ-Taxi application.

[12] During the course of the audit, we discussed and demonstrated the extent of the security exposure to OATH officials and provided a detailed list of exposed webpage links.

The DoITT *Application Development Policy* states that "All new systems must be tested in a separate environment for stability and to identify any unanticipated interactions with existing systems before they are moved to the production environment." The policy also directs that "All new systems must be tested for security integrity and functional verification prior to production release."

The access we were able to obtain indicates that there has been insufficient quality control during the development stage and inadequate system testing during the pre-release stage of the NYCServ-Taxi application.

NYCServ-Taxi's proper function is critical to the operations of OATH. It should not be available to unauthorized users who might be able to alter its content and reliability. Unauthorized access could facilitate fraudulent conduct and hinder its detection because malicious users could retrieve, insert, delete or modify data without logging into the application, and the application would not be able to track their activities. The impact of unauthorized access to administrator level functions is significant because by gaining access, a malicious internal user can establish fraudulent users on the system, damage application functions, and generally take control of the application. Due to the seriousness of the problem, we recommended that OATH immediately address the access vulnerability in the NYCServ-Taxi application during the course of the audit.

Recommendations

OATH should:

5. Remediate URL manipulation in the NYCServ-Taxi application in order to prevent unauthorized internal access.

OATH Response: "The ability to manipulate URLs to gain access *without any login* has been remediated, as have the server information that was appearing on certain error pages. . . . Remediation of URL manipulation by *logged-in individuals* is in progress currently. The agency is working to eliminate this issue entirely."

6. Restrict access to NYCServ-Taxi webpages with administrator level functions designed for management to authorized users only.

OATH Response: "Remediation of URL manipulation by *logged-in individuals* is in progress currently. The agency is working to eliminate this issue entirely."

7. Ensure against similar deficiencies in future application development projects by incorporating necessary steps into the Quality Assurance and Testing program.

OATH Response: The ability to manipulate URLs to gain access *without any login* has been remediated, as have the server information that was appearing on certain error pages. . . . Remediation of URL manipulation by *logged-in individuals* is in progress currently. The agency is working to eliminate this issue entirely."

Auditor Comment: The agency did not address this recommendation as written.

Personally Identifiable Information Exposed and Not Classified

Although OATH stated that all data in the NYCServ-Taxi application is public and that it does not contain PII, the NYCServ-Taxi application inadvertently records and stores certain PII such as, names, addresses, email addresses and telephone numbers of the summons' respondents and their representatives during the adjudication process. In addition, documents containing PII (such as drivers' licenses) were scanned into the NYCServ-Taxi application in order to identify certain individuals responding to summonses. We were able to access and download, in pdf form, all of this private information, including that which is PII. PII exposure has the potential to facilitate fraud, identify theft or other misuse. It violates an individual's expectancy of, and right to privacy.

The DoITT's *Data Classification Policy* states that "All information at the City of New York and corresponding agencies will be classified at one of four levels; public, sensitive, private, or confidential." It also states that "All personally identifiable information should be classified, at a minimum, as private." National Institute of Standards and Technology's *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[13] provides examples of PII data, such as social security numbers, driver's license numbers, and photographic images of persons.

OATH does not have a local operational policy to help guide its employees to alleviate the risk of collecting and storing PII into the NYCServ-Taxi application during summons adjudication hearings. However, OATH is responsible for protecting application data against unauthorized usage.

Recommendations

OATH should:

8. Comply with the DoITT Data Classification Policy to help guide employees to alleviate the risk of collecting and storing PII into the NYCServ-Taxi application.

OATH Response: "Data: NYCServ-Taxi does not contain any information that would be classified as 'private' (e.g., SSN), since it contains name and address information of respondents, which is generally something that is eligible for public release; the agency is obligated to disclose such data by FOIL request…. Its exposure present no adverse risk to the City, but rather a benefit…. Operationally, data such as name, address, license number (all of which are publically displayed. for example, in every NYC Taxi) are critical to the agency's adjudication and case management; it is not stored 'inadvertently,' as the report states, but rather as part of the performance of its mandated function."

Auditor Comment: National Institute of Standards and Technology Special Publication *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Section 2.2 identifies address information and driver's license numbers as PII. In addition, according to DoITT's Data Classification Policy, PII data must be classified at a minimum of "private" and handled accordingly. We encourage

[13] U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-122.

the agency to adopt the definition of PII as stated in NIST Special Publication 800-122 and respond appropriately to our audit recommendation.

9. Review the NYCServ-Taxi application data for PII and remove, block or shield the information from unauthorized disclosure.

OATH Response: "The ability to store a scanned image of a driver license is integral to the system's ability to facilitate hearings. The application is configured with security that restricts the viewing of scanned items to only those for whom such access is needed."

Auditor Comment: The audit revealed that role-based access control in NYCServ-Taxi application is not effective. Auditors were able to access and download representative data (including a scanned copy of their photo IDs) without having access privilege to view representative information.

10. Employ proper encryption methods to protect PII that is stored on the hard drives of computer systems or other network storage devices.

OATH Response: "Operationally, data such as name, address, license number (all of which are publically displayed. for example, in every NYC Taxi) are critical to the agency's adjudication and case management; it is not stored 'inadvertently,' as the report states, but rather as part of the performance of its mandated function. This data storage is not incidental to the web server management, but rather to OATH's established business practice."

Audit Comment: OATH did not directly address the recommendation in its response. In accordance with DoITT Data Classification Policy, all private data stored or transmitted must be encrypted.

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 in order to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the 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 focused on the NYCServ-Taxi application from its April 2012 inception through its operations in December 2015. We conducted audit fieldwork from September 2015 through December 2015. To achieve the audit objectives, we took the following steps:

- Reviewed the IT portion of OATH's 2013 and 2014 Financial Integrity Statement (Directive 1) for background information on systems-related issues at OATH;[14]
- Reviewed the TLC Rules and Local Laws that govern for-hire industries, as well as related businesses, in order to become familiar with the reasons associated with the issuances of summons, which are adjudicated by the TLT;
- Reviewed the TLT Rules in order to become familiar with the operations of the Tribunal;
- Reviewed OATH publications on TLT procedures in order to understand the summons hearing process;
- Reviewed contracts and task orders related to NYCServ-Taxi Application development to determine system specification and application development process;
- Interviewed OATH officials regarding the history of NYCServ-Taxi deployment, usage, and planned enhancements in order to understand the application specification and development process as well as future plans;
- Reviewed user manuals provided by the agency to understand the functions, features and user roles in the NYCServ-Taxi application;
- Reviewed the TLT adjudication workflow for handling violations to assist in our understanding of the Tribunal's usage of NYCServ-Taxi functions;
- Reviewed Mayor's Management reports for OATH and TLC and compared the summons data between two agencies;
- Sampled two weeks of the summons hearing schedule (one week each from July and August 2015) in order to understand the hearing volume, types of summons handled, and hearing location volume that would be processed through the NYCServ-Taxi application;
- Reviewed two weeks of the summons hearing schedule information from July and August, 2015, to analyze the summonses processed through NYCServ-Taxi, and the dispositions of the summons issued from reports generated by the application;
- Reviewed the implementation history of NYCServ-Taxi to assess the frequency and justification for changes made to the application;

[14] The Financial Integrity Statement (Directive 1) is submitted by various City agencies to the New York City Comptroller's Office on an annual basis.

- Analyzed software fixes applied to NYCServ-Taxi to determine whether the fixes are fully stabilized and are not re-occurring;
- Examined planned application work on NYCServ-Taxi to evaluate if the planned work represents necessary enhancements due to work process and/or business rule changes, or if the work was required to fix defects in NYCServ-Taxi functions or features;
- Reviewed NYCServ-Taxi configuration map information for details on the application deployment throughout OATH;
- Conducted walk-throughs of two major installations of NYCServ-Taxi for a better understanding of the work environment where the application is being used;
- Compared a listing of authorized users of NYCServ-Taxi against PMS data to determine if proper access levels were assigned to each user, and that only active employees are allowed to access the application;
- Tested the TLT summons hearing scheduling procedure by examining published scheduled hearings against information from the NYCServ-Taxi application to confirm that the published hearings were held as scheduled;
- Tested the reliability of summons adjudication data recorded into NYCServ-Taxi by a hearing officer as observed on September 29, 2015, and accessed NYCServ-Taxi on October 1, 2015, to confirm the accuracy of recorded information;
- Tested recorded audio files and its file association with adjudicated hearing cases to verify audio quality and their availability upon search request;
- Analyzed NYCServ-Taxi application system logs of users who accessed and processed information in the application;
- Performed an internal access security test and assessment on the NYCServ-Taxi application by testing user access to the application, both as an authorized user and as an unauthorized user;
- Reviewed and analyzed OATH's backup and disaster recovery plan for NYCServ-Taxi in the event of a system interruption;
- Reviewed the DoITT NYC *IT Security Policy* to determine if OATH is in compliance with the Policy;
- Obtained and reviewed the OATH-DoITT Service Level Agreement pertaining to DoITT's hosting of NYCServ-Taxi in order to evaluate the responsibilities and expectations of the parties;
- Obtained and reviewed the *DoITT Hosting Policy* to evaluate DoITT's policy in the hosting of City agency systems; and,
- Obtained and reviewed DoITT's *Operational Policy: DoITT Backup Retention* in order to evaluate DoITT's policy with regard to system backup.

CITY OF NEW YORK
OATH OFFICE OF ADMINISTRATIVE TRIALS AND HEARINGS

100 CHURCH STREET, 12TH FLOOR, NEW YORK, NEW YORK 10007

FIDEL F. DEL VALLE
COMMISSIONER AND CHIEF ADMINISTRATIVE LAW JUDGE
212-933-3001

June 8, 2016

By Hand Delivery
Majorie Landa
Office of the Comptroller
1 Centre Street, Room 1100
New York, NY 10007

RE: Audit Report on the Development and Implementation of the NYCServ-Taxi Administered by the Office of Administrative Trials and Hearings
S1115-122A

Dear Ms. Landa:

Attached please find a copy of OATH's response to the draft report on the Development and Implementation of NYCServ-Taxi.

If you require anything further, please contact this office.

Sincerely,

Fidel Del Valle, Esq.
Commissioner and Chief Administrative Law Judge

CITY OF NEW YORK
OATH OFFICE OF ADMINISTRATIVE TRIALS AND HEARINGS

100 CHURCH STREET, 12TH FLOOR, NEW YORK, NEW YORK 10007

FIDEL F. DEL VALLE
COMMISSIONER AND CHIEF ADMINISTRATIVE LAW JUDGE
212-933-3001

June 8, 2016

Office of the Comptroller
1 Centre Street, Room 1100
New York, NY 10007

Re: OATH Response to Comptroller's Audit Report SI15-122A

In response to the Comptroller's Audit Report for NYCServ-Taxi system, issued May 3, 2016, and to the exit conference, held May 12, 2016 at 66 John Street, 10th Floor, OATH hereby submits the following response, addressing each of the areas of remediation described by the Comptroller's Office in the report.

The Comptroller's recommendations fall into four categories:

I. Windows Password Complexity Not Enabled:

The agency's password security is enforced by DoITT – the agency's identity management, like that of many dozens of agencies, is hosted by DoITT. Any enforcement of password history, length, or complexity is a matter of DoITT policy. DoITT enforces password longevity: (i.e., re-use) as well as password length limits, but does not enforce the complexity aspect of the password policy. Although the agency can and do make recommendations regarding password security to users, OATH cannot enforce a policy if the host of the directory does not enforce it. DoITT's security team is aware of this discrepancy and will work with them to enable the complexity check, if possible.

II. Web server Security Updates Are Not Current

There have been numerous compatibility issues between the application code and the later version of the web server software. As a result, and because of competing priorities, this upgrade has been a long-term project, which is ongoing. OATH will upgrade to the latest web server version as soon as possible. OATH can also agree to a more pro-active maintenance practice for web server updates once the upgrade to the current version is complete.

III. Access Control Vulnerabilities in NYCServ-Taxi Application:

a. The ability to manipulate URLs to gain access *without any login* has been remediated, as have the server information that was appearing on certain error pages.

b. Remediation of URL manipulation *by logged-in individuals* is in progress currently. The agency is working to eliminate this issue entirely.

IV. Personally Identifiable Information Exposed:

a. Data:

NYCServ-Taxi does not contain any information that would be classified as "private" (e.g., SSN), It contains name and address information of respondents, which is generally something that is eligible for public release; the agency is obligated to disclose such data by FOIL request. OATH is currently working with City Hall to make it available for Hearings Division and For-Hire Vehicles on the Open Data Portal in the near future. Part of the assessment of the confidentiality of information is the determination of risk of damage resulting from exposure of this data. In this case, the City has determined (and has long held the view; the Open Data project dates back years) that such data is appropriate to share publically on a searchable database. Its exposure presents no adverse risk to the City, but rather a benefit.

Operationally, data such as name, address, license number (all of which are publically displayed, for example, in every NYC Taxi) are critical to the agency's adjudication and case management; it is not stored "inadvertently," as the report states, but rather as part of the performance of its mandated function. This data storage is not incidental to the web server management, but rather to OATH's established business practice.

b. Scanned images:

The ability to store a scanned image of a driver license is integral to the system's ability to facilitate hearings. The application is configured with security that restricts the viewing of scanned items to only those for whom such access is needed. From an application perspective, the code accommodates the need to keep scanned evidence safe from unauthorized access. In addition, the license image is something that drivers are required to display in a frame their vehicle for the public to see whenever they are working. The license is a public document necessary for any adjudication.

Additional Note:

Page 2: Correction: Currently, OATH staff manually enters dispositions into TAMIS. There is no nightly file produced by OATH.