



City of New York

OFFICE OF THE COMPTROLLER

Scott M. Stringer
COMPTROLLER



IT AUDIT

Marjorie Landa

Deputy Comptroller for Audit

Audit Report on the
Information System Controls of the
Domain Awareness System
Administered by the
New York City Police Department

7114-070A

June 26, 2015

<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 26, 2015

To the Residents of the City of New York:

My office has audited the New York City Police Department (NYPD) to determine whether the NYPD complies with its Public Security Privacy Guidelines (Guidelines) and whether it has adequate information system security controls over the Domain Awareness System (DAS). We perform audits of City agencies such as the NYPD as a means of ensuring that systems and technological resources of City agencies are efficient, secure and operating in accordance with applicable standards.

The audit found that the NYPD was in compliance with its Guidelines and in general had adequate security controls over its DAS information system. Specifically, the audit found that the NYPD had adequate procedures to ensure that DAS users were properly authorized, that they received the necessary privacy training before accessing the system, that videos were not available online beyond the required parameters, and that secondary use requests were required and reviewed to ensure that the NYPD had proper approval oversight for data usage. Further, as part of its DAS oversight, the NYPD conducted weekly meetings with its consultants and project administrators to provide system status updates and to coordinate system enhancements, such as software upgrades and installing additional cameras.

However, the audit also found certain user access control weaknesses. Specifically, the audit found that there were individuals with access rights to DAS who had not used the system for over three months. There also were individuals who were no longer NYPD employees whose DAS access had not been deactivated in the system. Further, the audit found that the Integrity Control Officers, who are responsible for monitoring DAS user activities, did not receive a standard set of criteria to use when reviewing DAS user activities and that the Integrity Control Officers had other responsibilities outside of DAS. Finally, the audit found some of the video cameras owned and operated by public and private entities that provide video feed to the NYPD had been offline over two years and some NYPD and non-NYPD video cameras were offline each month.

Based on the audit findings, we recommend that the NYPD periodically review the status of inactive user accounts and maintain an up-to-date user list; immediately disable the DAS access rights for all former employees; establish a standardized criteria for the Integrity Control Officers to use in reviewing DAS user activities; create a centralized oversight unit with staff only responsible for providing oversight of the DAS users to prevent misuse and misconduct; and consider potential ways to encourage public and private stakeholders to expedite the offline cameras' replacement or repair process.

The results of the audit have been discussed with NYPD 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 email my Audit Bureau at audit@comptroller.nyc.gov.

Sincerely,

A handwritten signature in blue ink, appearing to read "Scott M. Stringer", written over a printed name.

Scott M. Stringer

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
Audit Findings and Conclusions	1
Audit Recommendations.....	2
Agency Response.....	2
AUDIT REPORT	4
Background	4
Objectives.....	5
Scope and Methodology Statement.....	5
Discussion of Audit Results	5
FINDINGS AND RECOMMENDATIONS.....	7
User Access Control Weaknesses.....	7
Inactive Users Continue to Have System Access	8
Former Employees' Access Not Disabled	8
Information Security Monitoring Needs Improvement.....	9
Recommendations	9
Other Issue	10
Offline Cameras.....	10
Recommendation	11
DETAILED SCOPE AND METHODOLOGY.....	12
ADDENDUM	

THE CITY OF NEW YORK OFFICE OF THE COMPTROLLER IT AUDIT

Audit Report on the Information System Controls of the Domain Awareness System Administered by the New York City Police Department

7114-070A

EXECUTIVE SUMMARY

The audit was conducted to determine whether the New York City Police Department (NYPD) complies with its Public Security Privacy Guidelines and whether it has adequate information system security controls over its Domain Awareness System (DAS).

The NYPD enhances the quality of life in New York City (City) by working in partnership with the community and in accordance with constitutional rights to enforce the laws, preserve the peace, reduce fear and provide a safe environment for all residents and visitors to the City. Its Counter Terrorism Bureau works to guard against terrorism threats and includes the Lower Manhattan Security Initiative, a networked surveillance project designed to detect threats and perform preventive surveillance.

In 2007, the NYPD entered into a contract to develop DAS. Currently, DAS incorporates thousands of video cameras (including cameras installed by the NYPD and some belonging to other public and private entities) and hundreds of license plate readers. DAS also provides radiation and chemical alert support for environmental threats. This includes radiation detectors and chemical sensors. In addition, the NYPD has mobile cameras that provide supplemental coverage of short term special events, such as parades and marathons in the City.

NYPD established its Public Security Privacy Guidelines (Guidelines) to protect individual privacy in DAS and safeguard DAS data. The Guidelines also note that DAS cannot be used to target or monitor persons based on racial or religious profiling. The Guidelines further establish policies and procedures to limit DAS use and to provide for limited access to and proper disposition of stored data.

Audit Findings and Conclusions

Our audit found that the NYPD was in compliance with its Guidelines and in general had adequate security controls over its information system. Specifically, the NYPD had adequate procedures to ensure that DAS users were properly authorized, that they received the necessary privacy training before accessing the systems, that videos were not available online beyond the required

parameters, and that secondary use requests were required and reviewed to ensure that the NYPD had proper approval oversight for data usage. Further, as part of its DAS oversight, the NYPD conducted weekly meetings with its consultants, who provide system enhancements, program management quality assurance and maintenance support services for DAS, and with project administrators to provide system status updates and to coordinate system enhancements, such as software upgrades and installing additional cameras. In addition, the NYPD followed its Guidelines with regard to DAS video retention policies and procedures and the videos were not available online beyond the required parameters. Additionally, NYPD had effective policies and procedures to protect the privacy of information in DAS.

We did, however, find certain user access control weaknesses. Specifically, we found that there were individuals with access rights to DAS who had not used the system for over three months and some inactive users who had not accessed the system for more than one year. Finally, we found that there were individuals who were no longer NYPD employees whose DAS access had not been deactivated in the system. Furthermore, we reviewed DAS weekly usage for the three month period ending March 19, 2015, and noted that a consistent percentage of users did not access the system.

In addition, the NYPD has Integrity Control Officers who are responsible for monitoring DAS user activities. However, during the scope of the audit, we found that the Integrity Control Officers did not receive a standard set of criteria to use when reviewing DAS user activities and that the Integrity Control Officers had other responsibilities outside of the DAS system.

Finally, we found some of the video cameras owned and operated by public and private entities that provide video feed to the NYPD had been offline over two years. We also found that there were NYPD and non-NYPD video cameras offline each month. This is of concern because if offline or broken video cameras do not get reconnected, repaired or replaced as appropriate on a timely basis, DAS will not achieve its planned range of coverage.

Audit Recommendations

The NYPD should:

- Periodically review the status of inactive user accounts and maintain an up-to-date user list.
- Immediately disable the DAS access rights for all former employees.
- Establish a standardized criteria for the Integrity Control Officers to use in reviewing DAS user activities.
- Create a centralized oversight unit with staff only responsible for providing oversight of the DAS users to prevent misuse and misconduct.
- Consider potential ways to encourage public and private stakeholders to expedite the offline cameras' replacement or repair process.

Agency Response

The NYPD generally agreed with the report's findings and recommendations. However, the NYPD took exception with the audit finding that "[n]eglecting to deactivate User IDs for former users increases the vulnerability of DAS information." The NYPD in its response stated that the credentials for NYPD's computer network (known as "Finest") "are unique user names and

passwords issued to each member of the service or employee. Only after an employee's Finest credentials are validated, can an authorized user access DAS. At the conclusion of an employee's service, his or her Finest credentials are immediately invalidated. Consequently, a former employee would not even be able to access the Department network, let alone access DAS."

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

AUDIT REPORT

Background

As set forth in its mission statement, the NYPD enhances the quality of life in New York City by working in partnership with the community and in accordance with constitutional rights to enforce the laws, preserve the peace, reduce fear and provide a safe environment for all residents and visitors to the City. The NYPD's Counter Terrorism Bureau is charged with developing and implementing policies and procedures to guard against terrorism threats and includes the Lower Manhattan Security Initiative, a networked surveillance project designed to detect threats and perform preventive surveillance.

In 2007, the NYPD entered into a contract to develop DAS as an integrated surveillance system network designed to deter and detect terrorist attacks in the City. It includes license plate readers and video cameras owned and operated by the NYPD, as well as video cameras owned by other public and some private stakeholders. Public stakeholders include entities such as the City, New York State and federal agencies, and private stakeholders include entities such as banks and insurance companies. DAS provides the NYPD with data analysis support for monitoring suspicious activities at the Lower Manhattan Security Coordination Center.

In 2010, the NYPD awarded a contract to provide system enhancement, program management quality assurance and maintenance support services for DAS. The NYPD regularly meets with the project consultants who provide system enhancements, program management quality assurance and maintenance support services for DAS, and with team leaders to coordinate status updates and system enhancements, such as hardware and software upgrades and installing additional cameras. In addition, the participants in the weekly meetings discuss program timelines, program progress, security issues, and DAS account usage. These weekly meetings, which are documented in a series of regular reports, provide management controls over the monitoring and accountability for DAS by helping to ensure issues are addressed promptly.¹ In February 2015, the NYPD renewed a three-year contract for DAS system enhancement and expansion. It includes hardware and software upgrades, extending management quality assurance, and maintenance support services, as well as the lease for data centers. The NYPD also has an agreement with the Department of Information Technology and Telecommunications (DoITT) to provide additional disaster recovery services.

DAS draws data from the NYPD's Real Time Crime Center, which includes live data feeds of 911 calls, 311 calls, complaints, arrests and parking summonses issued. The system has the capability to access data from the New York Statewide Police Information Network and retrieve information from the New York State Department of Motor Vehicles. DAS also integrates the Metropolitan Transportation Authority cameras installed at select subway stations, and license plate readers at bridges and tunnels. DAS features include analytics search capacity that allows users to input specific searches. For example, a user could locate a vehicle and its owners within seconds by searching DAS data and the various linked databases. DAS also provides desktop alerts to notify NYPD personnel of potential threats and criminal activities.

DAS incorporates thousands of video cameras and hundreds of license plate readers. DAS also provides radiation and chemical alert support for environmental threats. This includes radiation

¹ The regular reports include multiple DAS report briefings.

detectors and chemical sensors. In addition, the NYPD has mobile cameras that provide supplemental coverage of short term special events, such as parades and marathons in the city.

NYPD established its Guidelines to protect individual privacy in DAS and safeguard DAS data. As the Guidelines note, “[T]he Domain Awareness System will be used only to monitor public areas and public activities where no legally protected reasonable expectation of privacy exists.” The Guidelines also mandate that DAS cannot be used to target or monitor persons based on racial or religious profiling. The Guidelines further establish policies and procedures to limit DAS’s use and to provide for limited access to and proper disposition of stored data. DAS users must complete a privacy training covering the proper use and handling of such information.

Objectives

The objectives of this audit were to determine whether the NYPD complies with its Public Security Privacy Guidelines and whether it has adequate information system security controls over DAS.

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, 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 2010 to March 2015. We conducted fieldwork from May 2014 to March 2015. It should be noted that tests of the public locations of the video cameras were outside the scope of this audit. 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 NYPD officials during and at the conclusion of this audit. A preliminary draft report was provided to NYPD officials and was discussed at an exit conference held on May 13, 2015. These discussions were considered in preparation of the draft report. Among other things, due to public safety concerns, NYPD officials requested, and we have agreed, that certain details they deem sensitive be deleted from the draft report and this final report. None of these details were material to our observations and they have not affected the validity of our audit findings. On June 1, 2015, we submitted a draft report to the NYPD with a request for written comments. NYPD submitted a written response to our draft report on June 15, 2015.

In its response to the draft report, with one exception, the NYPD generally agreed the report’s findings and recommendations. However, the NYPD disagreed with the audit finding that “[n]eglecting to deactivate User IDs for former users increases the vulnerability of DAS information.” NYPD officials stated that,

There is no stand-alone access to DAS. The DAS application can only be accessed via an NYPD computer connected to the NYPD network. In order for an authorized DAS user to access DAS, he or

she must first use his or her Finest credentials to log on to a Department computer. Finest credentials are unique user names and passwords issued to each member of the service or employee. Only after an employee's Finest credentials are validated, can an authorized user access DAS. At the conclusion of an employee's service, his or her Finest credentials are immediately invalidated. Therefore, it is virtually impossible for a former employee to access DAS.

Although NYPD believes it would be unlikely for a former employee to access DAS, NYPD has agreed to institute a process to immediately disable the DAS access to former employees. The full text of the NYPD's response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

Our audit found that the NYPD was in compliance with its Guidelines and in general had adequate security controls over its information system. Specifically, the NYPD had adequate procedures to ensure that DAS users were properly authorized, that they received the necessary privacy training before accessing the systems, that videos were not available online beyond the required parameters, and that secondary use requests were required and reviewed to ensure that the NYPD had proper approval oversight for data usage. Further, as part of its DAS oversight, the NYPD conducted weekly meetings with its consultants and project administrators to provide status updates and to coordinate system enhancements, such as software upgrades and installing additional cameras. The NYPD followed its Guidelines with regard to DAS video retention policies and procedures and video was not available online beyond the required parameters. Additionally, the NYPD had effective policies and procedures to protect the privacy of information in DAS.

We did, however, find certain user access control weaknesses. Specifically, we found that individuals with access rights to DAS had not used the system for over three months and that some users had not accessed the system for more than one year. Finally, we found that there were former employees whose user access had not been terminated. In addition, we reviewed DAS weekly usage for the three month period ending March 19, 2015 and noted that a consistent percentage of users did not access the system during that period of time. The NYPD should remove the access rights of those individuals who are no longer employees and consider re-assessing the access control rights to determine whether everyone who currently has access to DAS needs that access.

In addition, we found that the NYPD Integrity Control Officers who were responsible for monitoring DAS user activities did not receive a standard set of criteria to use when reviewing DAS user activities and that the Integrity Control Officers had other responsibilities outside of the DAS system. DAS needs a centralized oversight unit with a clear set of criteria to ensure that any DAS misuse and misconduct can be identified and addressed promptly.

Finally, we found that some of the video cameras owned and operated by other public and private entities that provided video feed to the NYPD have been offline over two years. We also found that there were NYPD and non-NYPD video cameras offline each month. This is of concern because if offline or broken video cameras do not get reconnected, repaired or replaced as appropriate on a timely basis, DAS will not achieve its planned range of coverage.

The above issues are discussed in detail below.

User Access Control Weaknesses

Each user is provided with a unique identification so that he or she is recognized and only then allowed access into the system. Adequate access controls and continual monitoring of user access help decrease the vulnerability of the system to misuse and abuse. As discussed below, our audit found that there were inactive DAS users whose access was not disabled, and that the NYPD did not ensure that DAS users who ceased to be employed by the NYPD no longer had system access.

Inactive Users Continue to Have System Access

To prevent misuse of the system information, user access accounts must be reviewed periodically. Our tests found DAS users identified as “active” who did not use the system for over three months and some who did not use the system for over a year. However, none of these seemingly inactive users were disabled from the system. Institution of adequate access controls and regular monitoring of user access would help ensure proper system operations.

Furthermore, we reviewed DAS weekly usage for the three month period ending March 19, 2015, and noted that a consistent percentage of users did not access the system. The NYPD should consider periodically re-assessing the access control rights to determine whether all these individuals need access to DAS.

Former Employees’ Access Not Disabled

According to DoITT’s Identity Management Security Policy, “[u]ser accounts will be created and de-provisioned in a timely manner.” Originally, only a limited number of NYPD personnel were intended to have DAS access. However, due to DAS’ expansion, more users have been added over time. The NYPD needs to strengthen its policies and procedures regarding user access controls to ensure that DAS user access receives periodic review and updates to permit only authorized, necessary users from logging into the system.

Neglecting to deactivate User IDs for former users increases the vulnerability of DAS information. The NYPD stated that none of the former employees have access into the NYPD’s systems after they have ceased employment. However, we have concerns that a former employee might still be able to gain access to DAS with his/her still active DAS credentials. Thus, there is potential vulnerability because the access rights were not deactivated.

To determine whether DAS User IDs belonged to authorized active employees, we compared the list of DAS users as of August 16, 2014, to the New York City Payroll Management System database. Our tests found that some users listed in the current DAS user list were retired, terminated or no longer active employees with the NYPD. Active password management should include deactivation of inactive user accounts or accounts for employees whose services have been terminated.

NYPD Response: “The NYPD disputes this finding because it disregards a fundamental aspect of DAS user access. There is no stand-alone access to DAS. The DAS application can only be accessed via an NYPD computer connected to the NYPD network. In order for an authorized DAS user to access DAS, he or she must first use his or her Finest credentials to log on to a Department computer. Finest credentials are unique user names and passwords issued to each member of the service or employee. Only after an employee’s Finest credentials are validated, can an authorized user access DAS. At the conclusion of an employee’s service, his or her Finest credentials are immediately invalidated. Consequently, a former employee would not even be able to access the Department network, let alone access DAS. Therefore, it is virtually impossible for a former employee to access DAS.”

Auditor Comments: Given that the NYPD’s current procedure is to notify the Office of Information Technology to deactivate an employee access upon separating from employment, but that the deactivation may take up to 24 hours, there remains a potential vulnerability when the access rights to DAS are not immediately deactivated. Further,

considering the increasing number of users who have been given DAS access, there is a greater security risk of system exposure if employees' access rights are not accurately monitored and maintained. An up-to-date user list is critical to verify whether a user is authorized and permitted to access sensitive information in DAS.

Information Security Monitoring Needs Improvement

According to the NYPD Patrol Guide, Integrity Control Officers are responsible for computer equipment and data security for all computer systems assigned to their command. Their responsibilities include monitoring and overseeing DAS user activities. However, our audit found that the Integrity Control Officers did not have standardized criteria for reviewing DAS user activities and that they were also assigned other responsibilities outside of the DAS system. Although the NYPD reported that DAS user activity reports were generated for the Integrity Control Officers to review in 2014, Integrity Control Officers were not required to regularly submit documentation to verify that they performed these reviews. The NYPD needs to ensure that its Integrity Control Officers properly perform their responsibilities to prevent misuse and misconduct over DAS.

Recommendations

The NYPD should:

1. Periodically review the status of inactive user accounts and maintain an up-to-date user list.

NYPD Response: “The NYPD understands the concern that is the basis of this recommendation; however, we believe that this recommendation is premature. The Department’s expansion of DAS beyond the Lower Manhattan Security Coordination Center did not begin until 2013 and took about one year to complete. The mobility initiative, which is currently underway, will place tablets in all Department vehicles and provide individual smart phones to members of the service. This initiative will make DAS available everywhere. With DAS accessible in the field, we anticipate that DAS usage will significantly increase. Because we want this powerful tool to be available to members of the service in case of an emergency, we do not want to terminate user rights due to sporadic use.”

Auditor Comment: Although the NYPD’s initiative will make DAS available to personnel everywhere, the NYPD would still need to ensure that DAS user list does not include former employees.

2. Immediately disable the DAS access rights for all former employees.

NYPD Response: “The NYPD agrees with this recommendation. The NYPD recognizes that managing user access is vital to DAS security. Currently, the NYPD manually controls user access rights, but we are building an automated process, which will integrate other employee management systems into DAS. When this integration is complete, any change in an employee’s status (transfer, termination, retirement, etc.) will be immediately reflected in DAS user controls.”

3. Establish a standardized criteria for the Integrity Control Officers to use in reviewing DAS user activities.

NYPD Response: “The NYPD agrees with this recommendation. The NYPD issued Interim Order 23 on February 6, 2015 that requires Integrity Control Officers to conduct a monthly audit of DAS usage. Interim Order 23 revises Patrol Guide 219-14 ‘Department Computer Systems,’ which details the Integrity Control Officers’ responsibilities to maintain the security and integrity of all Department computer systems and programs.”

4. Create a centralized oversight unit with staff only responsible for providing oversight of DAS users to prevent misuse and misconduct.

NYPD Response: “The NYPD agrees with the recommendation to have a centralized oversight unit for DAS; however, we do not agree with the recommendation to create a new unit. The Quality Assurance Division ‘QAD’ within the NYPD is already responsible for evaluating and overseeing compliance with the Department’s policies and procedures.” NYPD also stated that “[a]s a result of this recommendation, QAD will use the guidelines established in Interim Order 23 dated February 6, 2015 to create a self-inspection worksheet to be completed by every Integrity Control Officer on a monthly basis. The DAS audit will also be added as one of the performance areas that QAD evaluates on a quarterly basis. Any misuse or misconduct identified by the Integrity Control Officer or QAD will be referred to the Internal Affairs Bureau for further investigation.”

Auditor Comment: Although the NYPD recognizes the importance of closely overseeing DAS user activities, it does not believe that a separate unit is necessary. However, the NYPD should reconsider its position and create an independent oversight unit solely responsible for DAS.

Other Issue

Offline Cameras

The NYPD continually adds new video cameras to the DAS network as it expands the project across the City. As of March 2015, the NYPD had thousands of video cameras in the DAS network, which includes cameras operated by various public and private entities. The NYPD stated that during 2015, it will continue to add video cameras to the system. Among others, the NYPD expects to integrate the New York City Housing Authority video cameras into DAS.

Currently, most of the DAS video cameras are provided by public and private stakeholders. Relationships with stakeholders are governed by agreements with each of the public or private entities. As of March 19, 2015, we found that certain stakeholders’ video cameras had been offline for over two years. The NYPD stated that these cameras were offline due to Hurricane Sandy. Unless video cameras are reconnected, repaired or replaced on a timely basis, DAS monitoring coverage may be compromised. Although the NYPD regularly interacts with the stakeholders about cameras that are not operating properly, the NYPD also relies on stakeholders for repairs.

In addition, based on our review of the weekly briefings from January to March 2015, we found that there were NYPD and non-NYPD video cameras offline each month. It should be noted that there may be different cameras offline each week. According to the NYPD, these cameras had ceased operation due to power issues, construction, and camera breakage.

Recommendation

The NYPD should:

5. Consider potential ways to encourage public and private stakeholders to expedite the offline cameras' replacement or repair process.

NYPD Response: The NYPD generally agreed with this recommendation and stated that “[t]he NYPD understands this recommendation and has an automatic notification system in place as well as technical resources available to assist stakeholders with downed cameras. We make every effort to assist the stakeholder in getting the cameras back online. Every time a camera feed is lost, we automatically receive an alert in DAS. We immediately notify the stakeholder of the downed camera. These downed camera alerts are a unique benefit for stakeholders. In addition, we make our technical team available to assist stakeholders in re-establishing the camera connection. The NYPD has no authority, however, to repair or replace a stakeholder's private property.”

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, 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 2010 to March 2015. We conducted fieldwork from May 2014 to March 2015. It should be noted that tests of the public locations of the video cameras were outside the scope of this audit. To achieve our audit objectives, we:

- Interviewed various NYPD officials, including those from the NYPD's Office of Information Technology and its Counter Terrorism Bureau;
- Reviewed organization charts to gain an understanding of the administration of DAS;
- Conducted system walk-throughs of DAS to gain a better understanding of how NYPD DAS personnel perform their tasks and operations;
- Reviewed the DAS users' document and attended several DAS user training sessions to determine whether DAS users were properly trained to use the system;
- Reviewed the agreement between NYPD and stakeholders to determine whether the NYPD outlined the purposes for video camera, license plate reader data, and environmental data sharing procedures;
- Reviewed the agreements between the NYPD and stakeholders to determine whether NYPD specified procedures for equipment repairs;
- Reviewed the NYPD Guidelines to ensure that NYPD has adequate and effective controls to protect individual privacy;
- Reviewed and tested the retention policy as stated in the Guidelines to ensure videos were not available online beyond the required parameters;
- Reviewed video requests documentation to ensure that the NYPD has proper approval oversight for data sharing as specified in the Guidelines;
- Reviewed the Integrity Control Officers' roles and responsibilities as stated in the Guidelines to ensure the Integrity Control Officers conduct proper monitoring of DAS usage;
- Visited the Lower Manhattan Security Coordination Center to determine whether the NYPD has adequate physical security controls;
- Reviewed the DAS contracts and amendments to understand the project scope and the contractors' responsibilities;
- Reviewed the NYPD DAS documentation to understand the project scope and design of DAS;
- Reviewed the NYPD's policies and procedures to determine whether the NYPD has security controls in place;

- Reviewed the NYPD policies and procedures to determine whether the NYPD has adequate access controls;
- Attended several DAS report briefings from June 2014 to March 2015;
- Conducted field observations of scheduled camera maintenance and discussed procedures for emergency maintenance to determine whether the NYPD has adequate maintenance support services;
- Conducted license plate reader observations of bridges and tunnels in October 2014 to determine whether the license plate readers recorded information accurately;
- Conducted camera field observations at various locations within the City to ensure the cameras were operational;
- Reviewed the DAS documentation to determine whether the NYPD has documented approvals for new users;
- Compared the DAS user list as of August 16, 2014, to the Payroll Management System to test whether employees no longer working for the NYPD may still inappropriately have access to DAS;
- Determined whether NYPD user access controls complied with DoITT's Identity Management Security Policy and DoITT's Citywide Information Security Password Policy;
- Analyzed DAS user access controls to determine whether the NYPD deleted or disabled inactive users from the system;
- Reviewed documentation to determine whether the NYPD has a contingency plan in place in case of an emergency; and
- Reviewed the agreement between the NYPD and DoITT to provide additional disaster recovery services.



POLICE DEPARTMENT

JESSICA S. TISCH
DEPUTY COMMISSIONER

OFFICE OF INFORMATION TECHNOLOGY
ONE POLICE PLAZA – ROOM 900E
NEW YORK, N.Y. 10038

June 15, 2015

Marjorie Landa
Deputy Comptroller for Audit
Office of the Comptroller
1 Centre Street, Room 1100
New York, New York 10007

Re: Response to Draft Audit Report on the Information System Controls of the Domain Awareness System Administered by the New York City Police Department, 7114-070A

Dear Deputy Comptroller Landa:

I am responding to the Draft Report of an audit, which was conducted by the Bureau of Audit, New York City Comptroller's Office on the Information System Controls of the Domain Awareness System ("DAS"). The scope of this audit was from February 2010 to March 2015.

We are pleased that the Comptroller's Office found that the NYPD is in compliance with its *Public Security Privacy Guidelines* ("Guidelines"), which have the dual purpose of protecting the privacy rights of individuals engaged in public activities in public places; and providing security controls for access to and use of the information gathered and stored in the DAS database. We are satisfied with the finding that the NYPD has adequate procedures in place to ensure that DAS users are properly authorized and receive the necessary training in the privacy protocols prior to accessing the system. We appreciate the finding that the NYPD's management of the DAS includes weekly meetings with consultants and project administrators to provide status updates and to coordinate system enhancements. The NYPD's responses to the Comptroller's Office findings and recommendations are listed below.

The NYPD disagrees with the following finding:

1. "Neglecting to deactivate User IDs for former users increases the vulnerability of DAS information. The NYPD stated that none of the former employees have access into the NYPD's systems after they have ceased employment. However, we have concerns that a former employee might still be able to gain access to DAS with his/her still active DAS credentials." *Draft Audit Report, Page 6.*

Response: The NYPD disputes this finding because it disregards a fundamental aspect of DAS user access. There is no stand-alone access to DAS. The DAS application can only be accessed via an NYPD computer connected to the NYPD network. In order for an authorized DAS user to access DAS, he or she must first use his or her Finest credentials to log on to a Department computer. Finest credentials are unique user names and passwords issued to each member of the service or employee. Only after an employee's Finest credentials are validated, can an authorized user access DAS. At the

conclusion of an employee's service, his or her Finest credentials are immediately invalidated. Consequently, a former employee would not even be able to access the Department network, let alone access DAS. Therefore, it is virtually impossible for a former employee to access DAS.

The recommendations and the Police Department's responses are stated as follows:

1. **Recommendation:** The NYPD should periodically review the status of inactive user accounts and maintain an up to date user list.

Response: The NYPD understands the concern that is the basis of this recommendation; however, we believe that this recommendation is premature. The Department's expansion of DAS beyond the Lower Manhattan Security Coordination Center did not begin until 2013 and took about one year to complete. The mobility initiative, which is currently underway, will place tablets in all Department vehicles and provide individual smart phones to members of the service. This initiative will make DAS available everywhere. With DAS accessible in the field, we anticipate that DAS usage will significantly increase. Because we want this powerful tool to be available to members of the service in case of an emergency, we do not want to terminate user rights due to sporadic use.

2. **Recommendation:** Immediately disable the DAS access rights for all former employees.

Response: The NYPD agrees with this recommendation. The NYPD recognizes that managing user access is vital to DAS security. Currently, the NYPD manually controls user access rights, but we are building an automated process, which will integrate other employee management systems into DAS. When this integration is complete, any change in an employee's status (transfer, termination, retirement, etc.) will be immediately reflected in DAS user controls.

It is critical to understand, however, that as explained above, there is no stand-alone access to DAS. Instead, access by an NYPD employee to the DAS is a two-step process. Because an employee's unique Finest credentials are disabled at the conclusion of his or her service, a former employee would be unable to log on to any Department computer and thus, unable to access DAS. It is a misconception that neglecting to deactivate former employees' access increases the vulnerability of DAS information because it does not accurately reflect the technology in place.

3. **Recommendation:** Establish a standardized criteria for the ICOs to use in reviewing DAS user activities.

Response: The NYPD agrees with this recommendation. The NYPD issued Interim Order 23 on February 6, 2015 that requires Integrity Control Officers to conduct a monthly audit of DAS usage. Interim Order 23 revises Patrol Guide 219-14 "Department Computer Systems," which details the Integrity Control Officers responsibilities to maintain the security and integrity of all Department computer systems and programs.

According to Interim Order 23, which is attached to this letter, each Integrity Control Officer is required to select five members of the service at random who have access to the Domain Awareness System and review each selected member's activity, including video access activity, to ensure compliance with the Department's rules and regulations regarding computer systems. The results of this monthly inspection must be documented on typed letterhead and filed at the command. According to Patrol Guide 219-14, use of Department computer systems for personal or non-Department business matters is strictly prohibited and individuals who are found in violation of this policy will be subject to disciplinary action.

4. **Recommendation:** Create a centralized oversight unit with staff only responsible for providing oversight of DAS users to prevent misuse and misconduct.

Response: The NYPD agrees with the recommendation to have a centralized oversight unit for DAS; however, we do not agree with the recommendation to create a new unit. The Quality Assurance Division ("QAD") within the NYPD is already responsible for evaluating and overseeing compliance with the Department's policies and procedures. QAD's mission is to emphasize a commitment to the quality and excellence of the NYPD. QAD currently evaluates each command's compliance in over 25 performance areas. QAD audits four performance areas every quarter or audit cycle and the four performance areas are rotated every audit cycle. QAD also creates self-inspections to be completed by the Integrity Control Officers within a command.

As a result of this recommendation, QAD will use the guidelines established in Interim Order 23 dated February 6, 2015 to create a self-inspection worksheet to be completed by every Integrity Control Officer on a monthly basis. The DAS audit will also be added as one of the performance areas that QAD evaluates on a quarterly basis. Any misuse or misconduct identified by the Integrity Control Officer or QAD will be referred to the Internal Affairs Bureau for further investigation.

5. **Recommendation:** The NYPD should consider potential ways to encourage public and private stakeholders to expedite the offline cameras replacement or repair process.

Response: The NYPD understands this recommendation and has an automatic notification system in place as well as technical resources available to assist stakeholders with downed cameras. We make every effort to assist the stakeholder in getting the cameras back online. Every time a camera feed is lost, we automatically receive an alert in DAS. We immediately notify the stakeholder of the downed camera. These downed camera alerts are a unique benefit for stakeholders. In addition, we make our technical team available to assist stakeholders in re-establishing the camera connection. The NYPD has no authority, however, to repair or replace a stakeholder's private property.

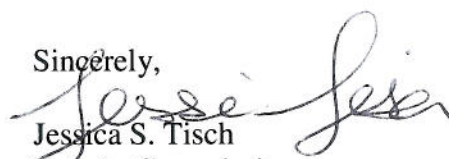
We understand the auditors' concern that downed cameras affect some DAS coverage. First, it is important to note that the downed cameras reported in the weekly briefings referenced by the auditors are not a cumulative count of all downed cameras in a particular week. Instead, a report is run at a specific time during the week, e.g., Tuesday

at 10:00am, which shows the downed cameras at that particular moment in time. This number of downed cameras is continually changing, as cameras are constantly being brought back online. Secondly, in the event of a consistent camera outage in a sensitive location, the NYPD has the ability to deploy mobile cameras to restore camera coverage.

The Comptroller's Office noted that a number of stakeholder cameras have been offline for over two years. These cameras are owned by two stakeholders who suffered massive infrastructure damage during Hurricane Sandy. Once the damage is repaired and the cameras are back online, the NYPD will re-integrate these cameras into DAS.

We appreciate the auditors' time and effort to complete this audit. The auditors were very thorough in their assessment. We value the recommendations offered by the Comptroller's Office. If you have any questions concerning this response, please contact Director Courtney MacGregor at (646) 610-6169.

Sincerely,



Jessica S. Tisch
Deputy Commissioner,
Information Technology



INTERIM ORDER

SUBJECT: REVISION TO PATROL GUIDE 219-14, "DEPARTMENT COMPUTER SYSTEMS"		
DATE ISSUED:	REFERENCE:	NUMBER:
02-06-15	P.G. 219-14	23

1. In order to ensure the integrity of all Department computer systems, Patrol Guide 219-14, "Department Computer Systems" is being revised to require Integrity Control Officers to conduct a monthly audit of the Domain Awareness System.

2. Therefore, effective immediately, Patrol Guide 219-14, "Department Computer Systems" is amended as follows:

- a. **ADD** new step "19", opposite actor "INTEGRITY CONTROL OFFICER", on page "2" to read:

"INTEGRITY CONTROL OFFICER"

- 19. Conduct a monthly audit of the Domain Awareness System.**
- a. Select five members of the service at random who have access to the Domain Awareness System.**
 - b. Review each selected member's activity, including video access activity, to ensure compliance with the Department's rules and regulations regarding computer systems.**
 - c. Document results of monthly inspection on Typed Letterhead and file at command.**

3. Upon publication, this Interim Order has been incorporated into the On-Line Patrol Guide.

4. Any provisions of the Department Manual or any other Department directive in conflict with the contents of this Order are suspended.

BY DIRECTION OF THE POLICE COMMISSIONER

**DISTRIBUTION
All Commands**