City of New York

OFFICE OF THE COMPTROLLER

Scott M. Stringer
COMPTROLLER

AUDITS AND SPECIAL REPORTS

IT AUDIT

Marjorie Landa

Deputy Comptroller for Audit

Audit Report on the New York City Department of Citywide Administrative Services' Access Controls over Its Computer Systems

SI17-085A

June 27, 2017

http://comptroller.nyc.gov

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

June 27, 2017

To the Residents of the City of New York:

My office has audited the Department of Citywide Administrative Services (DCAS) to determine whether it has adequate system security and access controls in place to protect information in its computer environment. We perform audits of this type of the information technology (IT) systems maintained by City agencies such as DCAS to help ensure the integrity of the data stored in those systems and to minimize the risk of improper access to the City's systems.

The audit found that DCAS has established adequate controls for application access, data protection, and sufficient data classification guidelines to protect information in the agency's computerized environment. However, our audit found weaknesses in DCAS' access and security controls. Specifically, the audit found that user access had not been disabled for inactive users and former City employees. In addition, we found that DCAS' list of agency liaisons—designated officials in other City agencies responsible for authenticating those agencies' users and their roles in relation to one of DCAS' mission-critical, multi-agency application—had not been adequately monitored and updated. Further, we found that DCAS did not implement and enforce the City Department of Information Technology and Telecommunications' (DoITT) password expiration and complexity rules that are intended to allow only authorized users to gain access to City IT systems. Finally, we found that DCAS lacks a formal agency-wide business continuity plan and a disaster recovery plan for its applications. Currently, DCAS is unable to provide business continuity for its mission-critical applications.

Based on the audit findings, we made 10 recommendations including that DCAS should: ensure that all former and inactive employees' accounts are immediately disabled; maintain an up-to-date external user list to properly monitor its network user accounts; develop a password policy and procedure for its applications that complies with DoITT standards to prevent the risk of unauthorized access; develop a formal business continuity plan and consider developing a disaster recovery plan for its mission-critical applications.

The results of the audit have been discussed with DCAS 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 New York City Department of Citywide Administrative Services' Access Controls over Its Computer Systems

SI17-085A

EXECUTIVE SUMMARY

This audit was conducted to determine whether the New York City Department of Citywide Administrative Services (DCAS) has adequate system security and access controls in place to protect information in its computer environment.

DCAS performs a wide range of administrative functions for other New York City government agencies. Among other things, DCAS supports City agencies' personnel needs; designs and administers civil service exams; manages City-owned buildings; procures goods and services; and manages City vehicles. In Fiscal Year 2016, it had 2,179 employees.

To meet its varying responsibilities, DCAS maintains a computer network that is used by DCAS employees, consultants and interns for email and to access department files. It also maintains specialized applications that are used by the public, DCAS network users (employees, interns and consultants), and personnel in external City agencies. Several applications maintained by DCAS contain confidential and private information. To ensure the requisite level of security, it is essential that DCAS maintain adequate access controls, such as user-authorization, identification, authentication, access-approval and login credentials. DCAS is responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment.

Audit Findings and Conclusions

The audit found that DCAS has established adequate controls for application access, data protection, and sufficient data classification guidelines to protect information in the agency's computerized environment. However, we found weaknesses in DCAS' access and security controls. Specifically, user access had not been disabled for inactive users and former City employees, which could increase security risks. In addition, DCAS' list of agency liaisons—designated officials in other City agencies responsible for authenticating those agencies' users and their roles in relation to one of DCAS' mission-critical, multi-agency application—had not been adequately monitored and updated. Further, DCAS did not implement and enforce the City

Department of Information Technology and Telecommunications' (DoITT's) password expiration and complexity rules that are intended to allow only authorized users to gain access to City IT systems.

Finally, DCAS lacks a formal agency-wide business continuity plan and a disaster recovery plan for its applications. Currently, DCAS is unable to provide business continuity for its mission-critical application, Direct Order Online. DCAS anticipates resolving that issue by migrating the application from the DCAS data center to DoITT by April 2018. DCAS is vulnerable to the loss of mission-critical information in the case of a catastrophic event or emergency until the issue is resolved.

Audit Recommendations

To address these issues, we make 10 recommendations to DCAS:

- Ensure all former and inactive employees' accounts are immediately disabled and that periodic reviews are conducted to identify and deactivate the accounts of former employees.
- Develop a process that regularly reviews user activity, identifies inactive users, and disables inactive accounts promptly.
- Maintain an up-to-date external user list to properly monitor its network user accounts.
- Reassess its current list of Direct Order Online users to ensure that each user is currently authorized and needs access.
- Immediately communicate with each City agency that uses the Direct Order Online application to update their liaison information.
- Develop a procedure to ensure that the identities of Direct Order Online liaisons are promptly updated by the City agencies when changes occur.
- Develop a password policy and procedure for its applications that complies with DoITT standards to prevent the risk of unauthorized access.
- Periodically perform vulnerability scans for its applications to reduce potential threats.
- Assign a manager who will be responsible for scheduling scans and ensuring that vulnerability tickets are reviewed, remediated, and closed.
- Develop a formal business continuity plan and consider developing a disaster recovery plan for the mission-critical applications that are within DCAS data center pending their anticipated migration to DoITT.

Agency Response

DCAS agreed with nine of the audit recommendations and partially agreed with one recommendation to reassess the current list of Direct Order On-Line user access.

AUDIT REPORT

Background

DCAS performs a wide range of administrative functions for City government and had 2,179 employees as of Fiscal Year 2016. Among other functions, DCAS supports City agencies' personnel needs; designs and administers civil service exams; provides training programs; manages City-owned buildings; leases and sells real estate; procures goods and services; establishes and pays utility accounts; implements energy conservation programs; and manages City vehicles.

To meet its varying responsibilities, DCAS maintains a computer network used by DCAS employees, consultants and interns to gain access to department emails and files. It also maintains specialized applications that are used by the public, DCAS network users (employees, interns and consultants), and personnel in external City agencies. These specialized applications include:

- Direct Order Online for Citywide procurement services;
- Online Application System for Civil Service examinations; and
- FleetFocus to manage and track the maintenance of City vehicles.

These applications and others maintained by DCAS contain confidential and private information. According to the DoITT Citywide Information Security Policy, information stored in an agency's applications must be placed in a secured environment and protected from unauthorized access. To accomplish that level of security, adequate access controls, such as user-authorization, identification, authentication, access-approval and login credentials are essential. DCAS is responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment, including by complying with DoITT’s polices.

As the City agency charged with overseeing information technology (IT) and telecommunications for more than 120 City agencies, DoITT provides assistance to help the agencies deliver efficient, effective and secure IT services. It provides security expertise and services and seeks to protect City data and IT assets through proper management of security infrastructure, policies, and standards. All City agencies and employees, as well as contractors and vendors doing business with the City, are required to follow those policies and standards.

Objectives

To determine whether DCAS has adequate system security and access controls in place to protect information in its computer environment.

Scope and Methodology Statement

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, 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 October 1, 2016 to April 30, 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 DCAS officials during and at the conclusion of this audit. A preliminary draft report was sent to DCAS and was discussed at an exit conference on May 26, 2017. The discussions with DCAS and its submission of additional information were considered in preparation of this draft report. On June 6, 2017, we submitted a draft report to DCAS with a request for written comments. We received a written response from DCAS on June 20, 2017.

In its response, DCAS agreed with nine of the audit recommendations and partially agreed with one recommendation to reassess the current list of Direct Order On-Line user access. With regard to that recommendation, DCAS stated, "As determining which staff require access to Direct Order Online or serve as liaisons within each agency is the responsibility of the respective agency, DCAS will request that user agencies review their current lists of users and liaisons and confirm or update the information." Since DCAS is responsible for maintaining and monitoring the Direct Order Online application, we urge the agency to proactively communicate with each agency on a regular basis regarding user access changes to ensure that only authorized users have access to Direct Order Online.

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

FINDINGS AND RECOMMENDATIONS

The audit found that DCAS has established adequate controls for application access, data protection, and sufficient data classification guidelines to protect information in the agency's computerized environment. However, we found weaknesses in DCAS' access and security controls. Specifically, user access had not been disabled for inactive users and former City employees, which could increase security risks. In addition, DCAS' list of agency liaisons—designated officials in other City agencies responsible for authenticating those agencies' users and their roles in relation to one of DCAS' mission-critical, multi-agency applications—had not been adequately monitored and updated. Further, DCAS did not implement and enforce DoITT's password expiration and complexity rules intended to allow only authorized users to gain access to City IT systems.

Finally, DCAS lacks a formal agency-wide business continuity plan and a disaster recovery plan for its applications. Currently, DCAS is unable to provide business continuity for its mission-critical application, Direct Order Online. DCAS anticipates resolving this issue by migrating the application from DCAS data center to DoITT by April 2018. DCAS is vulnerable to the loss of mission-critical information in the case of a catastrophic event or emergency until this issue is resolved.

Inappropriate Access to the Network

Through our audit testing, we found that DCAS did not ensure that access to its network was promptly deactivated for former employees and inactive users, i.e., employees on long-term leave and individuals who had not logged into the network for 90 days or more. DCAS is responsible for creating, monitoring, and disabling access to its network when the status of a network user changes.[1] DoITT's Identity Management Security Policy states that "[u]ser accounts will be created and de-provisioned in a timely manner." Comptroller's Directive #18 section 8.1.2 requires the "[d]eactivation of inactive user accounts and accounts for employees whose services have been terminated."

We reviewed and analyzed a list of 1,935 DCAS network user accounts that were active as of January 19, 2017 and found that DCAS had not deactivated the accounts of 196 network users who had not logged into the network for periods of over 90 days to one year. In addition, we found that 32 users listed in the City's Payroll Management System (PMS) as former employees or employees on long-term leave had access to the network.

Moreover, according to DCAS records, 9 out of the 32 former or inactive employees had logged into the network *after* they left DCAS. It also appears that two of those nine user accounts were created six to sixteen years after the named users' DCAS employment ceased. Specifically, network identification (ID) was created in August 2014 in the name of an individual who left DCAS employment in August 1998 and City employment in June 2009, and that ID was used to access the network in December 2016. In the second case, a user ID assigned to a former employee who left City employment in August 2007 was created in August 2013 and was used to access the network as recently as January 2017.

At the exit conference, DCAS officials informed us—and subsequently provided an email from a DCAS contractor stating in substance—that the network user accounts for the two former City

[1] A network user can be an employee, a consultant, or an intern.

employees referenced in the preceding paragraph were created after they left City employment and were retained by the contractor as consultants (Fire Safety Directors). However, we note that neither individual was on the list of authorized consultants that DCAS provided during the audit. To properly monitor its network user accounts DCAS, should ensure that its lists of authorized external users, such as consultants, are up to date.

DoITT policy mandates that "[u]sers must be positively and individually identified and validated prior to being permitted access to any City computing resource." Without properly authenticating that users are authorized to have access and removing the access of departing employees promptly, DCAS is at risk of someone's gaining unauthorized access to its network and agency information.

> ***Agency Response:*** "As part of its efforts to bridge the digital divide, DCAS created user accounts for custodial staff and other staff that do not have daily access to computers. In furtherance of those efforts, DCAS relaxed its deactivation policy to allow these staff to retain uninterrupted access to the network. As a result of the audit, DCAS will revise its policies and procedures to include the identification and deactivation of staff on long-term leaves. Additionally, DCAS will perform routine comparisons of user information to PMS data."

Outdated Lists of City Agencies' Liaisons and External Users of DCAS' Direct Order Online Application

We found that DCAS does not ensure the accuracy of its list of City agency liaisons—individuals employed by other City agencies who are authorized to request that DCAS provide access to its Direct Order Online application.

DCAS' mission-critical application, Direct Order Online, allows City agencies to create, review, approve and submit orders against DCAS contracts through New York City's intranet (which is separate and distinct from DCAS' network). To use that application, City employees in agencies other than DCAS must request access through their designated City agency liaisons. DCAS depends on each agency's liaison to (1) validate the identities of that agency's users as agency employees with responsibilities related to ordering, and (2) notify DCAS to create and disable their accounts when warranted.

We found that of the 169 agency liaisons for 95 City agencies on DCAS' current list, 35 liaisons for a total of 31 agencies, no longer work for those agencies. Those individuals are still authorized, as far as DCAS is concerned, to request online access for employees of agencies where the liaisons no longer work. In addition, in as many as 8 of the 31 City agencies, DCAS may not have a current, active agency liaison identified who is responsible to monitor and inform DCAS of relevant changes in the employment status of those agencies' employees with access to DCAS' online ordering application.

Currently, approximately 84 percent of the 2,202 users of the Direct Order Online accounts are external to DCAS (that is, employed by other City agencies). DCAS' Online Direct Order System User Guide indicates that "[a]gencies designate approval authority levels for staff." Based on our review of 100 user accounts, we found that 21 percent of those users could not be found in PMS as working for the assigned agency and so presumably had left their agencies. Without proper monitoring to ensure that only authorized users have access to the Direct Order Online application, its security, the integrity of its data, and its controls to protect the City against the risk of unauthorized transactions being conducted through the application may be compromised.

Agency Response: "The auditors stated that DCAS does not ensure the accuracy of Direct Order users and liaisons. Firstly, it is unclear whether the auditors' sample size of 4.7% of users is representative of the population. Secondly, as was communicated to the auditors, it has always been the responsibility of the user agencies to update user and liaison information and transmit this information to DCAS. Nonetheless, DCAS will contact the user agencies and request that they confirm or update the information."

Auditor Comment: Our audit found that DCAS' reliance on the user agencies to update user and liaison information did not result in an up-to-date list. Therefore, we are pleased that DCAS has agreed to contact the user agencies and request that they confirm or update the information.

Recommendations

DCAS should:

1. Ensure all former and inactive employees' accounts are immediately disabled and that periodic reviews are conducted to identify and deactivate the accounts of former employees.

   Agency Response: DCAS agreed with this recommendation.

2. Develop a process that regularly reviews user activity, identifies inactive users, and disables inactive accounts promptly.

   Agency Response: DCAS agreed with this recommendation.

3. Maintain an up-to-date external user list to properly monitor its network user accounts.

   Agency Response: DCAS agreed with this recommendation.

4. Reassess its current list of Direct Order Online users to ensure that each user is currently authorized and needs access.

   Agency Response: DCAS partially agreed with this recommendation, stating, "As determining which staff require access to Direct Order Online or serve as liaisons within each agency is the responsibility of the respective agency, DCAS will request that user agencies review their current lists of users and liaisons and confirm or update the information."

   Auditor Comment: Given the fact that DCAS is the application owner for the Direct Order Online, it should not depend solely on each agency to notify it of user access changes. We urge DCAS, as part of reassessing the current list of Direct Order Online users, to actively communicate with each agency on a regular basis to ensure that only authorized users have access.

5. Immediately communicate with each City agency that uses the Direct Order Online application to update their liaison information.

   Agency Response: DCAS agreed with this recommendation.

6. Develop a procedure to ensure that the identities of Direct Order Online liaisons are promptly updated by the City agencies when changes occur.

   Agency Response: DCAS agreed with this recommendation.

System Security Control Weaknesses

We found security weaknesses such as inadequate password complexity and lack of password expiration protocols. In addition, DCAS does not periodically perform vulnerability scans of its applications. Proper security controls over systems and continual monitoring reduces system vulnerability to security breaches as well as opportunity for misuses.

Lack of Password Controls

We found that DCAS' password controls do not always conform to applicable DoITT standards. Specifically, we found three DCAS critical applications did not comply with DoITT's password complexity and expiration rules. A strong password lowers the risk of unauthorized access to any electronic information system. Password strength is a measure of the effectiveness of a given password in preventing an unauthorized individual from successfully guessing that password. The strength of a password is determined by its length and complexity. DoITT password policy states that, "[p]asswords 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."

DCAS has policies and procedures to protect its network against unauthorized access. However, we found, the password policies for two of DCAS' mission-critical applications, Direct Order Online and Storehouse Online, lack the required provisions for password-complexity and length. In addition, the user is allowed an unlimited number of failed attempts to log into both applications. As a result, those applications may be vulnerable to unauthorized access and misuse. DoITT's Citywide Information Security Policy states that "[a]ll passwords and personal identification numbers (PINs) used to protect City of New York systems shall be appropriately configured, periodically changed, and issued for individual use." The DoITT policy specifically requires that "[a]ll accounts which provide access to SENSITIVE, PRIVATE OR CONFIDENTIAL information must be automatically disabled after a maximum of five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes." [Emphasis in original.]

DCAS also does not comply with DoITT's policy mandating that passwords must be changed every 90 days, or with Comptroller's Directive #18, Section 8.1.2, which requires that "users [should be] forced to change passwords periodically." Specifically, we found that DCAS' Direct Order Online and Storehouse Online applications currently allow the use of passwords that never expire. Further, neither application disables a user account until it has been inactive for 210 days.[2] In addition, we found that DCAS' FleetFocus application does not comply with DoITT's 90-day password expiration policy. DCAS explained that the password expiration feature for FleetFocus needs to be manually entered by the administrator, and informed us that the agency has taken corrective action to rectify that condition. Inadequate password controls may increase the potential threat of unauthorized access.

[2] Both applications notify users through email when an account has been dormant for 180 days and then allow an additional 30-day grace period before the account is automatically deactivated.

Agency Response: "DCAS has already effected a 90-day password expiration policy on its Fleet Focus system. Due to the complexity of the upgrades needed for the Direct Order and Storehouse Online applications, DCAS will need to hire a consultant in order to make those systems compliant. DCAS expects to complete this effort by quarter two of 2018."

DCAS Does Not Periodically Perform Vulnerability Scans

A vulnerability scan can help analyze, identify, and classify security weakness and threats to an organization's network and applications. However, we found DCAS does not perform vulnerability scans to identify security weaknesses and threats to the servers located in the DCAS data center. DCAS officials explained that although the agency does not perform proactive vulnerability scans it responds to instances of suspicious activities.

The DCAS servers located in the data center house the Direct Order Online application and the Storehouse Online application, which are mission-critical applications for DCAS. They also house other non-mission-critical systems.[3] The Citywide Vulnerability Management Policy requires all agencies to proactively protect information systems from vulnerabilities and reduce the potential for exploitation of information. As suggested by DoITT, agency security and information technology personnel are encouraged to perform regular vulnerability scans using McAfee Vulnerability Manager (MVM).

According to DoITT's Vulnerability Management Standard, "[a]ll City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." It further states, "[a]t least one agency business unit manager must be assigned who will be responsible for scheduling scans and ensuring that vulnerability tickets are review, remediated, and closed." Without periodic vulnerability scans DCAS applications may be at risk of security breaches.

Recommendations

DCAS should:

7. Develop a password policy and procedure for its applications that complies with DoITT standards to prevent the risk of unauthorized access.

   Agency Response: DCAS agreed with this recommendation.

8. Periodically perform vulnerability scans for its applications to reduce potential threats.

   Agency Response: DCAS agreed with this recommendation.

9. Assign a manager who will be responsible for scheduling scans and ensuring that vulnerability tickets are reviewed, remediated, and closed.

   Agency Response: DCAS agreed with this recommendation.

[3] DoITT performs routine scans of the DCAS servers that are hosted at a DoITT site.

DCAS Lacks Business Continuity Plan and Disaster Recovery Plan

DCAS does not have a formal agency-wide business continuity plan or a disaster recovery plan. A business continuity plan identifies the processes and procedures an organization must put in place to ensure that mission-critical functions can continue during and after a disaster. As a component of a comprehensive business continuity/disaster recovery plan, the plan should specify the steps that need to be taken to quickly resume agency operations without material loss of computer data in the event of emergency or system failure. At the exit conference, DCAS explained that there would be no material loss of computer data because DCAS backs up its data. However, DCAS stores daily and weekly backup data on site and only sends monthly backup tapes to an off-site facility. Therefore, the daily and weekly data could be lost in case of an emergency in the building where they are stored.

Without an adequate agency-wide business continuity plan and a disaster recovery plan, DCAS is vulnerable to the loss of mission-critical information and operational ability in the event of a disaster, emergency or system failure. Comptroller's Directive #18, Section 10 states that "[a] formal plan for the recovery of agency operations and the continuation of business after a disruption due to a major loss of computer processing capability is an important part of the information protection plan. The increasing dependence on computers and data processing support makes it ever more critical for Agency Heads to focus on this area."

Currently, DoITT is responsible for disaster recovery for certain of DCAS' mission-critical applications hosted at DoITT's site, such as Archibus used by DCAS for facilities management. DCAS officials said that they are working on migrating five other critical applications, including Storehouse Online, from the DCAS data center to DoITT. DCAS anticipates the process of migrating those applications to DoITT to begin by the fourth quarter of 2017. Once the migration is completed, DoITT will be responsible for the disaster recovery for the applications.

Nonetheless, DCAS does not have a business continuity plan for its mission-critical application, Direct Order Online. DCAS explained that this application will also be migrated to DoITT. However, because of the current application's design, it is unable to migrate at present. DCAS is in a process of obtaining a contract to rewrite the application and update the database and estimates that the Direct Order Online will be migrated to DoITT April 2018.

Recommendation

DCAS should:

10. Develop a formal business continuity plan and consider developing a disaster recovery plan for the mission-critical applications that are within DCAS data center pending their anticipated migration to DoITT.

    Agency Response: DCAS agreed with this recommendation.

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 October 1, 2016 to April 30, 2017. We conducted fieldwork from November 2016 to April 2017. To achieve our audit objectives, we:

- Reviewed the DCAS Organization Chart to gain an understanding of the administration of DCAS units;
- Interviewed DCAS officials in the IT department, Human Capital Unit, Procurement Unit, City Record Unit, Energy Unit, Fleet Unit, and Asset Management Unit to understand the services provided by each unit;
- Conducted system walk-throughs for critical applications to gain an understanding of service operations through these applications;
- Analyzed and reviewed DCAS applications that are in production to determine whether DCAS has adequate access controls to prevent unauthorized access;
- Reviewed DCAS documentation to determine whether it has policies and procedures in place for creating new users and terminating the accounts of inactive users;
- Determined whether DCAS applications' user access controls complied with Comptroller's Directive #18 and DoITT's Identity Management Standard, Identity Management Security Policy, and Password Policy;
- Reviewed DCAS' Comptroller's Directive #1 submission to determine whether DCAS has proper internal controls;
- Reviewed documentation to determine whether DCAS has adequate security controls over its computer environment;
- Reviewed and analyzed documentation to determine whether DCAS has controls in place to monitor system violations and intrusions;
- Conducted access control tests such as password format, length, and complexity. Performed tests to determine whether DCAS disables user access after five sequential invalid login attempts within 15 minutes, and has lock out feature for after 15 minutes of inactivity;
- Obtained and reviewed a list of 1,935 network users (external and internal) including user name, user ID, account creation date, last logon date, and agency information;
- Compared DCAS network users list as of January 19, 2017 to the City's PMS to test whether users no longer working for DCAS may still inappropriately have access to the network and whether these user access were removed in a timely manner;
- Analyzed the network user list to determine whether inactive users' access were disabled;

- Examined the Direct Order Online agency liaison list to determine whether DCAS maintains an accurate list;
- Compared the current Direct Order Online agency liaison list with PMS to determine whether they are active employees;
- Reviewed the Direct Order Online active user list to determine whether DCAS monitor user status;
- Randomly selected 100 users from the list of 2,202 active Direct Order Online users and performed test with PMS to determine whether these users are active employees;
- Reviewed documentation to determine whether DCAS has policies and procedures for data classification, data protection, and record retention;
- Reviewed documentation regarding DCAS system migration to DoITT to understand the project scope and timeline; and
- Reviewed IT operations policy and procedure, backup policy, and disaster recovery protocol to determine whether DCAS has controls in place to support business continuity in case of an emergency.

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

Citywide Administrative Services

Lisette Camilo
Commissioner

The David N. Dinkins
Municipal Building
1 Centre Street
New York, NY 10007

212 386 0201 tel
nyc.gov/dcas

June 20, 2017

Ms. Marjorie Landa
Deputy Comptroller for Audit
Office of the New York City Comptroller
1 Centre Street, RM 1100
New York, NY 10007

RE: NYC Comptroller's Audit Report on the Department of Citywide Administrative Services' Access Controls over Its Computer Systems, Audit No. SI17-085A

Dear Deputy Comptroller Landa:

Thank you for the opportunity to respond to the audit report on the Department of Citywide Administrative Services' Access Controls over its Computer Systems. I am pleased that the audit found that DCAS has established controls for application access, data protection, and data classification guidelines to protect information in the Agency's computerized environment.

Below are our responses to the findings and recommendations:

FINDINGS

Finding 1: Inappropriate Access to the Network

DCAS Response:
The auditors stated that 196 of 1,935 users had not logged in to the network for periods of over 90 days, but remained as active users on the network. Additionally, the auditors identified 32 users that they claimed were not found in the City's Payroll Management System (PMS) or were on long-term leaves.

As part of its efforts to bridge the digital divide, DCAS created user accounts for custodial staff and other staff that do not have daily access to computers. In furtherance of those efforts, DCAS relaxed its deactivation policy to allow these staff to retain uninterrupted access to the network. As a result of the audit, DCAS will revise its policies and procedures to include the identification and deactivation of staff on long-term leaves. Additionally, DCAS will perform routine comparisons of user information to PMS data.

Finding 2: Outdated Lists of City Agencies' Liaisons and External Users of DCAS's Direct Order Online Application

DCAS Response:

The auditors stated that DCAS does not ensure the accuracy of Direct Order users and liaisons. Firstly, it is unclear whether the auditors' sample size of 4.7% of users is representative of the population. Secondly, as was communicated to the auditors, it has always been the responsibility of the user agencies to update user and liaison information and transmit this information to DCAS. Nonetheless, DCAS will contact the user agencies and request that they confirm or update the information.

Finding 3: Lack of Password Controls

DCAS Response:

As the auditors stated, DCAS has policies and procedures to protect its network against unauthorized access. However, two of DCAS's 79 applications (Direct Order and Storehouse Online) lack the password-complexity required by DoITT and three applications, (Direct Order, Storehouse Online and Fleet Focus), are not compliant with the password expiration policy. DCAS is aware of these issues and work is underway to correct them. DCAS has already effected a 90-day password expiration policy on its Fleet Focus system. Due to the complexity of the upgrades needed for the Direct Order and Storehouse Online applications, DCAS will need to hire a consultant in order to make those systems compliant. DCAS expects to complete this effort by quarter two of 2018.

Finding 4: DCAS Does Not Periodically Perform Vulnerability Scans

DCAS Response:

Although vulnerability scans were not being performed, DCAS has safeguards in place to ensure that DCAS is not at risk of security breaches. DCAS has McAfee anti-virus installed on all the servers hosted in DCAS data center and DCAS has installed CrowdStrike on all desktops and servers to protect and prevent against Ransomware type of attacks. Also, DOITT's Security Operation Council (SOC) monitors all of the City's networks, including the servers in DCAS Data center, to maintain their confidentiality, integrity and availability. DCAS has already appointed a manager and modified the policy to perform annual vulnerability scans for all the applications hosted in DCAS data center.

Finding 5: DCAS Lacks Business Continuity Plan and Disaster Recovery Plan

DCAS Response:

Although DCAS does not have formal written Business Continuity or Disaster Recovery Plans for the 8 applications hosted in DCAS' data center, DCAS is not at risk of losing mission critical information. DCAS backs up its data on a daily basis in two ways: DCAS backs up its data onto tapes which are retained by its data archive vendor and also backs up its data onto disks which are stored at DoITT.

RECOMMENDATIONS

The auditors made ten recommendations as follows:

Recommendation 1: Ensure all former and inactive employees' accounts are immediately disabled and that periodic reviews are conducted to identify and deactivate the accounts of former employees.

Recommendation 2: Develop a process that regularly reviews user activity, identifies inactive users, and disables inactive accounts promptly.

Recommendation 3: Maintain an up-to-date external list to properly its network user account

Recommendation 4: Reassess its current list of Direct Order Online users to ensure that each user is currently authorized and needs access.

Recommendation 5: Immediately communicate with each City agency that uses the Direct Order Online application to update their liaison information.

Recommendation 6: Develop a procedure to ensure that the identities of Direct Order Online liaisons are promptly updated by the City agencies when changes occur.

Recommendation 7: Develop a password policy and procedure for its applications that complies with DoITT standards to prevent the risk of unauthorized access.

Recommendation 8: Periodically perform vulnerability scans for its applications to reduce potential threats.

Recommendation 9: Assign a manager who will be responsible for scheduling scans and ensuring that vulnerability tickets are reviewed, remediated, and closed.

Recommendation 10: Develop a formal business continuity plan and consider developing a disaster recovery plan for the mission-critical applications that are within DCAS data center pending their anticipated migration to DoITT.

DCAS agrees with recommendations 1 through 3 and 5 through 10. DCAS partially agrees with recommendation 4. As determining which staff require access to Direct Order Online or serve as liaisons within each agency is the responsibility of the respective agency, DCAS will request that user agencies review their current lists of users and liaisons and confirm or update the information.

DCAS is committed to ensuring the protection and control of its data and its information processing resources. We will use the information provided by this audit to further strengthen DCAS' internal control environment.

Sincerely,

Lisette Camilo