FOLLOW-UP OF

COMPUTER USER IDS

REPORT NO. 09-05-107F

City of Albuquerque
Office of Internal Audit and Investigations

City of Albuquerque

Office of Internal Audit and Investigations
P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

September 30, 2009

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico

Follow-Up: Computer User IDs
09-05-107F

FINAL

INTRODUCTION

The Office of Internal Audit and Investigations (OIAI) performed a follow-up of Management Audit No. 05-107, Computer User IDs, issued June 28, 2006. The purpose of our follow-up is to report on the progress made by Department of Finance and Administrative Services/Information Systems Division (DFAS/ISD) management in addressing our findings and recommendations.

The City of Albuquerque (City) protects its data and computer systems by using access controls to identify users, restrict access, and monitor activity on the City's network and applications. Computer user IDs and passwords are used to authenticate or verify that persons attempting to gain access to City computer resources are valid City employees. Controls regarding appropriate use and administration of computer User IDs and passwords can help reduce risk of unauthorized access to City data. DFAS/ISD is responsible for the administration of these controls for centrally managed systems. The initial audit evaluated City Information Technology (IT) policies, procedures, and standards pertaining to the use and administration of user IDs and passwords.

SCOPE, OBJECTIVES, AND METHODOLOGY

Our follow-up procedures consist of interviews of City personnel and review and verification of applicable documentation to assess the status of our audit recommendations. Our follow-up is substantially less in scope than an audit. Our objective is to ensure management has taken meaningful and effective corrective action in regards to our findings and recommendations.

We conducted this performance audit in accordance with generally accepted government auditing standards. This audit was also conducted in accordance with IT Governance Institute's Control Objectives for Information and related Technology (CobiT) audit guidelines. The IT Governance

Institute is a standard setting organization for information systems auditing. 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.

The scope of the follow-up did not include an examination of all the functions and activities related to DFAS/ISD. We limited our scope to actions taken to address our audit recommendations from the date of our final report, June 28, 2006 to July 6, 2009.

RECOMMENDATION NO.1

The 2006 audit determined that DFAS/ISD was not promptly notified when an employee was terminated, transferred, or was found to be involved in inappropriate or illegal activities. There were no written instructions requiring department supervisors to contact DFAS/ISD immediately to have a departing employee's computer access disabled.

OIAI tested a sample of terminated employees to determine if their computer user access was revoked in a timely manner. Testing revealed that 97% of employees sampled did not have their access revoked in a timely manner.

OIAI recommended that the CAO ensure that a process and policy be developed requiring all City departments to promptly notify DFAS/ISD in writing when a departing employee's computer access needed to be revoked.

The CAO responded and agreed that DFAS/ISD should be promptly notified when a departing employee's computer access should be terminated. The CAO would work with the Human Resources Department (HRD) to ensure departmental Human Resources (HR) Coordinators were tasked with the responsibility of notifying DFAS/ISD when any employee was terminated or transferred.

ACTION TAKEN

The recommendation has not been implemented.

In January 2009, the City replaced its financial and human resource systems with PeopleSoft, an Enterprise Resource Planning (ERP) system. PeopleSoft HRMS is the human resource/payroll module of this system.

- HRD is exploring the functionality of the "notify" capability in PeopleSoft HRMS which may allow DFAS/ISD to be automatically notified when a termination action is entered into the system. If testing is successful this step will be added to the HR checklist for the termination process.
- HRD has discussed the Employee Clearance Form and termination process in HR Coordinators meetings. In the response to our follow-up memo it was stated that the Employee Clearance Form was updated in September 2006. This form was updated, but Section 4c pertaining to computer access cancellation or its corresponding instructions was not modified.
- In May 2009, during this follow-up audit HRD automated the generation of weekly terminations reports, these reports are emailed to the Help Desk. These reports also include temporary employees which were excluded in previous termination reports.

OIAI performed test work to determine if improvements have been made regarding the timeliness of user access revocation for terminated employees. OIAI defined timely as within 24 hours of an employee's termination date. We chose a statistical sample of 39 out of a total of 365 employees who were terminated from July 1, 2008 to May 14, 2009. Thirty eight out of 39 employees (97%) tested did not have computer access revoked in a timely manner. DFAS/ISD did not receive notification of termination for six employees in our sample. These employees still have access to City computer resources. The majority of termination notifications are obtained from termination reports.

RECOMMENDATION

The CAO should ensure that all City departments promptly notify DFAS/ISD in writing when a departing employee's computer access needs to be revoked.

RESPONSE FROM CAO

"The City Employee Clearance Record Instructions Section 4c clearly makes the employee's supervisor responsible for terminating computer access "with a service request or an e-mail message to the ISD Help Desk." The CAO and Human Resources Department will reinforce the appropriate handling of the clearance process with Department Directors, HR Coordinators and supervisors.

"The automated terminated employees report sent to ISD is intended only to be an additional check in the process, since the report reflects terminations once they are entered into the HRMS system after an employee's final paycheck has

> ***cleared. The report is valuable; however, in identifying employees whose access should be terminated at departure is clearly more effective and immediate at the department level."***

RECOMMENDATION NO. 2

The DFAS/ISD User ID Security Policy stated "User IDs shall not be shared among users" and "unique user IDs of a standard format, with passwords, shall be required to access all multi-user computer systems."

OIAI surveyed City departments regarding compliance with IT policies and standards and determined that policies and procedures regarding appropriate use of computer user IDs were not always followed.

OIAI recommended the CAO ensure that IT technology policies and standards were periodically communicated to employees.

The CAO responded and agreed that IT policies and standards should be periodically communicated to employees. IT policies, standards and procedures are available on the City intranet, are reviewed and updated as necessary by the Information Systems Committee (ISC).

In August 2006, DFAS/ISD planned to implement an IT certification process that would be used to communicate DFAS/ISD policies, standards, and procedures.

ACTION TAKEN

The audit recommendation has been fully implemented.

In 2006 DFAS/ISD implemented the IT Certification Program, also referred to as IGivetest, to periodically communicate DFAS/ISD policies, standards, and procedures and test employees' knowledge. All City technology users are required to take the test within 30 days of their hire date and annually thereafter.

OIAI discussed the IGivetest program procedures with DFAS/ISD. Employees are notified by DFAS/ISD to take the test within 30 days of their hire or anniversary date. If employees neglect to take the test their computer access is revoked. DFAS/ISD maintains a database of employees who have requested computer access which is updated daily with information from HRD and from the DFAS/ISD Help Desk system.

OIAI reviewed the information and questions on the IT Certification test and noted that guidance on appropriate use of computer user IDs and passwords is covered in the test.

RECOMMENDATION NO. 3

DFAS/ISD management informed OIAI that they were aware that City employees hide their computer system passwords in locations where others may find them.

OIAI recommended the CAO ensure that City employees were periodically informed about safeguarding of computer system passwords. This could be done by creating a policy that requires employees to safeguard computer system passwords.

The CAO responded and agreed that safeguarding of passwords was an important aspect of an IT security policy. The City IT User ID Security Policy stated "User IDs and passwords shall not be shared among users". The CAO was hopeful that the annual IT security certification process would make users more aware of this fundamental safeguard.

ACTION TAKEN

The audit recommendation has been fully implemented.

OIAI reviewed the questions and information provided in the IT Certification test (discussed in Recommendation No. 2) and determined that guidance on appropriate use of user IDs and passwords is covered on the test.

RECOMMENDATION NO. 4

DFAS/ISD management informed OIAI that it did not monitor unsuccessful logins to City computer systems and that there was not staff available within the City to monitor login activity.

The City IT User ID Security Policy stated, "Unsuccessful access attempts and access violations shall be automatically logged, reported, and reviewed by the System Administration function for appropriate follow-up."

OIAI recommended that DFAS/ISD always monitor and investigate unsuccessful logins.

DFAS/ISD responded and agreed that "high value" unsuccessful logins such as on system administrator and application administrator accounts should be investigated. However, the vast majority of unsuccessful logins were typically the result of a forgotten password. With automated account lockout controls, reactivation required the user to contact the DFAS/ISD Help Desk for account reactivation. The sheer volume of successful logins per day, numbering in the thousands, precluded meaningful active monitoring of this activity.

ACTION TAKEN

The audit recommendation has been resolved.

In the response to OIAI's follow-up memo, DFAS/ISD stated that a series of unsuccessful login attempts from one location to multiple systems would be investigated if encountered.

The User ID Security Policy, that formed the basis of the recommendation, was recently revised and policy item #11 was removed, which stated: "Unsuccessful access attempts and access violations shall be automatically logged, reported, and reviewed by the System Administration or Security Administration function for appropriate follow-up". Since DFAS/ISD network and system administrators do not perform this activity it was taken out of the policy. This policy revision was approved by the Technology Review Committee (TRC) on June 18, 2009 and is expected to be presented to the ISC, at the September 2009 meeting, with the recommendation to approve.

To determine if threats exist on the City network DFAS/ISD utilizes Cisco's Monitoring, Analysis, and Response System (MARS). OIAI observed MARS and discussed it's capabilities in regards to detecting unauthorized intrusions with the DFAS/ISD Network Manager. While MARS is not an intrusion detection system it has the capability to analyze user behavior to determine if a possible threat exists. MARS will also recommend a course of action to mitigate the threat. One of the benefits of this system is that information is in real-time and threats can be addressed in a timely manner. MARS aggregates and analyzes millions of pieces of information, one of which is login activity, and presents the information in graphical or report format. Network performance and high level incidents are reviewed on a daily basis by network administrators. MARS is a compensating control that can provide useful and timely information regarding threats to the City's systems.

RECOMMENDATION NO. 5

The City IT User ID Standard required user IDs to consist of six alphabetic characters, combining a three-character prefix and a three-character suffix. OIAI tested user IDs for compliance with this standard. Five (8%) of the 60 user IDs tested were not in compliance with this standard and were generic user IDs. Generic or shared user IDs were not granted to an individual but could be used by multiple employees which preclude tracking of transactions to a specific employee.

The DFAS/ISD User Security Policy Exception Procedure requires departments that need shared/generic user IDs to submit a written request to be reviewed and approved by the TRC.

OIAI recommended that the CAO require all departments needing to establish shared/generic user IDs to follow the DFAS/ISD User ID Security Policy Exceptions Procedure.

The CAO responded and agreed that departments needing shared/generic user IDs for valid business purposes should comply with the appropriate IT policies, standards and procedures.

In June 2006 all departments identified as having generic user IDs were notified of the User ID Security Policy Exception procedures and were advised to begin the process to obtain the exception. Departments were advised that all generic user IDs would be automatically disabled unless the department had taken action to retain the use of the generic user IDs.

ACTION TAKEN

The audit recommendation has been partially implemented.

OIAI reviewed a list of 87 generic IDs as of May 14, 2009 and compared them to the 32 generic IDs approved for exception and determined that 75 generic IDs (86%) were not on the approved exceptions list.

In May 2009 DFAS/ISD started a clean up of generic user IDs. Many of these user IDs were no longer used and some accessed systems that are no longer in use. DFAS/ISD notified departments that had generic user IDs and requested them to submit a written request and to attend the June 18, 2009 TRC meeting to justify their request. At this TRC meeting generic user IDs were approved for Council Services, Environmental Health, Fire, and Parks and Recreation Departments. Generic user IDs for Cultural Services, Family & Community Services, and Parks & Recreation Departments were deferred until a future TRC meeting because additional information was necessary or no department representatives were present.

The City IT standard "Approved Exceptions to User ID Security Policy" was revised to include new generic user IDs that were approved, or scheduled to be reviewed by the TRC. This revised standard is scheduled to be reviewed and approved by the TRC once all of the generic user ID requests are addressed.

The City IT User ID Standard was revised April 19, 2007 to consist of six characters. Each user ID has a one character alpha prefix followed by a five digit numeric suffix. The prefix is used to denote the type of employee: E=City employee, W=Albuquerque Bernalillo County

Water Utility Authority, and X=external parties (vendors and subcontractors). Employees hired prior to April 19, 2007 still retain the old format.

RECOMMENDATION

DFAS/ISD should ensure that departments have complied with the City IT User ID Security Policy Exceptions Procedures prior to granting a generic ID.

RESPONSE FROM DFAS/ISD

"The ISD Help Desk staff has been trained that no generic IDs will be created unless approval is first obtained from the Technical Review Committee (TRC). The Help Desk procedures will be updated to include instructions on dealing with generic ID requests."

RECOMMENDATION NO. 6

The City IT Novell Netware Login Password Standard (Novell Password Standard) required passwords to be in the following format:

- *Exactly* 8 characters
- No vowels
- At least 1 number
- At least 1 capital letter
- At least 1 special character: !, @, #, $, %, ^, &, *, (,)

DFAS/ISD personnel informed OIAI that the parameters had not been activated on the Novell network to match the format specified in the Novell Password Standard. A module needed to activate password parameters would cost approximately $120,000. Due to the expense, ISC decided to configure Novell to lockout a user after three attempts with an invalid password.

OIAI recommended that DFAS/ISD change the Novell Password Standard to require a *minimum* of eight characters, and a combination of alpha and numeric characters.

DFAS/ISD responded and agreed with the recommendation. DFAS/ISD would continue to investigate cost-effective password control options including, but not limited to, additional Netware components, third party products, password synchronization products and the replacement of Novell Netware.

ACTION TAKEN

The audit recommendation has been fully implemented. DFAS/ISD revised the Novell Password Standard on May 15, 2008 to require a *minimum* of eight characters, a numeric, an upper case character, and a special character.

RECOMMENDATION NO. 7

The City IT User ID Security Policy stated that a standard shall be published detailing specifications for passwords, including: expiration intervals; lockout after a standard number of access attempts with an incorrect password; not permit the re-use of prior passwords for a minimum standard number of iterations; automatically terminate a user session after a minimum standard period of inactivity; and a system shall provide an audit trail of transactions performed identifying the user, date, time, transaction, and data accessed or altered.

OIAI tested eight City systems identified by DFAS/ISD for user ID and password security. OIAI reviewed system parameters to verify:

- Passwords were set to expire after a predefined interval or deactivated after a period of non-activity.
- A standard number of unsuccessful attempts were required before lockout.
- Re-use of prior passwords was prohibited.
- An audit trail of transaction activity was created.

OIAI's test work of the eight systems indicated the following:

- Four did not have the password set to expire at a predefined interval and five did not have the user IDs set to deactivate after a predefined interval of non-use.
- Four were set to inhibit the use of a user ID after a standard number of access attempts with an incorrect password.
- Three did not limit the re-use of prior passwords for a standard number of iterations.
- Three did not provide an audit trail of transactions.

OIAI recommended that DFAS/ISD management ensure that user ID and password controls are in place for accessing City systems.

DFAS/ISD responded and agreed with the recommendation. While some systems were incapable of enforcing all rules, DFAS/ISD would investigate options to synchronize passwords and enforce common password control attributes.

ACTION TAKEN

The recommendation has been fully implemented. A valid user ID and password is required to access all centrally managed systems.

OIAI reviewed password settings of nine centrally managed systems. Five of the systems were previously tested in 2006 and four of the systems were implemented after 2006. It was determined that all nine systems require a user ID and password to access but not all follow best practice guidance. Some systems do not have the capability to set specific password settings such as prohibiting the reuse of prior passwords, enable complexity, or deactivate a user after a specific period of inactivity.

DFAS/ISD is in the process of revising the User ID Security Policy to address limitations of existing systems. The revision was approved by the TRC on June 18, 2009 and is expected to be presented at the September 2009 ISC meeting with a recommendation to approve. Policy items #9 and 10 have been modified. The following are the revised items, the text in red was added as part of the revision:

9. A system, **when capable**, shall automatically terminate a user session after a minimum standard period of inactivity.
10. A system, **when capable**, shall provide an audit trail of transactions performed identifying the user who initiated the transaction, the date and time of the transaction, type of entry, and what data was accessed or altered. This information shall be retained for a minimum standard time period, notwithstanding additional retention periods, which may be mandated by other policies or by law.

RECOMMENDATION NO. 8:

CobiT recommended enforcing separation of duties to help avoid the subversion of critical processes by a single individual.

OIAI inquired and observed the duties of security and system administrator for eight City computer systems. OIAI determined that security and system administrative functions were not separated for four systems.

OIAI recommended that DFAS/ISD management ensure that there was a separation of duties between system administration and security functions for all City computer systems.

DFAS/ISD responded and agreed in principle with the recommendation. Major line of business applications, such as finance, payroll, the new PeopleSoft billing (CIS) and Constituent Relationship Management (CRM) systems, had clear separation between system administration and application security functions. In addition, the Domino email security administrators were separated from the UNIX system administrators. However, this approach was not practical when the underlying system and the service offered was one in the same, such as Novell Netware or Windows file sharing. However, DFAS/ISD would continue to split the responsibilities where it was prudent to do so.

ACTION TAKEN

The recommendation has been resolved. There appears to be a separation of duties in place for the ability to initiate, authorize, execute, and verify transactions as recommended by CobiT.

OIAI reviewed user ID management procedures with DFAS/ISD personnel for nine centrally administered systems for the setup and administration of user IDs and determined that a separation of duties exists for the following:

- Authorization for system and application access is performed by an employee's supervisor. Initiation and authorization for user access is the same procedure. Access to centrally managed applications need to be approved by the business owner of the application.
- The execution or setup of user security privileges is performed by system administrators for each application. Type of access is based upon the supervisor and business owner authorization.
- The execution of business transactions within applications is performed by department users. DFAS/ISD system administrators do not have access to process transactions within centralized business applications.
- The verification of business transactions is performed within each department, not in DFAS/ISD.

System and security administration of operating systems such as Novell and Active Directory are usually performed by the same individual since these systems do not process business transactions but are platforms that business applications run on.

Separation of duties for the user account management appears to be adequate for centrally managed business applications.

RECOMMENDATION NO. 9:

DFAS/ISD required all Help Desk personnel to positively identify all individuals requesting the reset of their computer systems passwords. DFAS/ISD Help Desk personnel positively identified the individuals by requesting the last four digits of their Social Security Number (SSN), mother's maiden name, or favorite color.

A sample of City employees contacted the DFAS/ISD help desk to request the reset of their computer system passwords. Two employees sampled had their passwords reset, but were not positively identified.

OIAI recommended that DFAS/ISD management ensure that all Help Desk representatives positively identify everyone who requests their password to be reset and to formalize the positive identification requirement as part of the IT Policies and Standards.

DFAS/ISD responded and agreed with the recommendation. They would stress to the DFAS/ISD Help Desk staff the importance of and the established requirement for validating an individual's identity before resetting passwords.

ACTION TAKEN

The recommendation was partially implemented.

DFAS/ISD created the Password Verification Procedure which contains instructions for Help Desk personnel to confirm the identity of individuals by verifying the last 4 digits of the caller's SSN. DFAS/ISD Help Desk personnel were trained on the procedures.

OIAI selected a sample of ten City employees who called the DFAS/ISD Help Desk to have their password reset for various centrally managed systems. In five of ten requests DFAS/ISD Help Desk personnel did not ask for the caller's last four digits of their SSN. DFAS/ISD Help Desk personnel asked for the caller's name and user ID or employee number to verify their identity.

RECOMMENDATION

DFAS/ISD should ensure that Help Desk personnel positively identify users in accordance with the Password Verification Procedure.

RESPONSE FROM DFAS/ISD

"To address this issue, ISD is currently implementing Advanced Software Products Group's ReACT password reset software. ReACT is designed to automate the password reset and synchronization process across the entire enterprise. It will eliminate the need to reset a password to a temporary value. ReACT allows the end users to reset their own passwords at any time without the need to change their password again at sign-on. This product should significantly reduce the password reset related calls to the Help Desk.

"Additionally, ISD will instruct the fairly new Help Desk staff on the appropriate password verification procedures."

ADDITIONAL FINDINGS NOTED DURING THE FOLLOW-UP

The following findings were noted during our test work and were not part of the original audit. The following findings concern areas that we believe could be improved by the implementation of the related recommendations.

1. THE CAO SHOULD ENSURE THAT DFAS/ISD IS NOTIFIED OF ALL EMPLOYEE, VENDOR, AND SUBCONTRACTOR TERMINATIONS SO THAT COMPUTER ACCESS IS PROMPTLY REVOKED.

   Employees are coded as active in the payroll systems after they have left the City either through termination or early retirement. These employees do not show up on termination reports. This was a problem with the previous payroll system termination reports and is still an issue with reports from PeopleSoft HRMS. An employee is active until all payments have been made. Payments may include their final paycheck, accrued vacation, and deferred compensation. If an employee takes early retirement he or she is coded as active until full payment is received. During this time the employee is not listed on the termination reports and could have access to City computer systems. HRD personnel stated that employees are coded as active for a minimum of two weeks after they have left the City.

   The current process of relying on the employee's supervisor or department HR coordinators to notify the Help Desk of terminations is not working effectively. According to DFAS/ISD personnel about 15% of departments currently contact the Help Desk for termination notification. The DFAS/ISD Help Desk relies on the termination reports for this information but these reports are not adequate for timely notification.

Currently there are no formal procedures to address the revocation of computer access for non-City employees. Vendors and subcontractors are not included in termination reports and often DFAS/ISD is not notified of their departure from the City.

If computer user access is not promptly revoked, the risk of unauthorized access increases. Unauthorized access could lead to compromised City data and systems or disclosure of sensitive information.

CobiT's control objective for identity management addresses the maintenance of user IDs. This objective states that organizations should ensure that a timely information flow is in place that reports changes in jobs (i.e. people in, people out, people change). Organizations should grant, revoke, and change user access rights in coordination with human resources and user departments for users who are new, who have the left the organization, or have changed roles or jobs.

RECOMMENDATION

The CAO should ensure that DFAS/ISD is notified of terminations either on or before the termination date for City employees, vendors and subcontractors. Procedures such as the use of the "notify" function within PeopleSoft HRMS (as mentioned in the Action Taken section of Recommendation No. 1 on page 2) could be used for timely notification of the DFAS/ISD Help Desk for City employees. In addition, exit procedures should be developed for vendors and subcontractors to ensure those with user IDs have their computer access revoked.

RESPONSE FROM CAO

"The CAO and Human Resources Department will reinforce the appropriate handling of the clearance process with Department Directors, HR Coordinators and supervisors. The "notify" function within PeopleSoft was explored by HRD and determined that the function is tied to the entry of the termination action in the HRMS system. As stated above, terminations cannot be entered into the HRMS system until the employee's final paycheck has been processed. The "notify" function is therefore no timelier than the automated termination report.

"The CAO agrees that exit procedures should be developed for vendors and subcontractors and will ask HRD to work with Legal, DFAS and City departments in the development and implementation of these procedures."

2. DFAS/ISD SHOULD ENSURE THAT EMPLOYEES WHO DO NOT TAKE THE IT CERTIFICATION TEST HAVE THEIR COMPUTER ACCESS DISABLED.

During the June 2009 TRC meeting it was noted that computer access privileges were not being revoked for employees not taking the IT Certification test. Due to turnover in the Help Desk area and limited personnel resources this had been overlooked. DFAS/ISD has plans to address this issue and will be notifying all employees who are not in compliance. These employees will be required to take the test within a specified time frame or lose their computer access privileges.

Employees who do not take the IT Certification Test may not be aware of technology policies and procedures that will make their data more secure by:

- Keeping their passwords confidential
- Saving City data on network drives
- Using the Internet and email appropriately

The Employee IT Security Certification Policy states that each employee who has been issued access credentials shall complete the certification process within 30 days of the date of the request for access, then annually within 30 days of the employee's anniversary date.

RECOMMENDATION

DFAS/ISD should implement procedures to ensure that all employees who do not take the IT Certification test within the specified time frame have their computer access disabled.

RESPONSE FROM DFAS/ISD

"DFAS/ISD agrees and will implement the Employee IT Security Certification policy. A list of the personnel overdue in taking the test will be provided to each department by September 21, 2009, giving the departments a final chance to become compliant. On October 5, 2009, ISD will deactivate all user accounts for the delinquent employees. Every month thereafter, accounts will be deactivated for all employees who have failed to take the certification test."

3. DFAS/ISD SHOULD CHANGE THE NOVELL NETWARE PASSWORD SETTINGS TO MATCH THE NOVELL NETWARE LOGIN PASSWORD STANDARD, WHEN CAPABLE.

DFAS/ISD implemented Recommendation No. 6, on page 8, which was to revise the Novell Netware Login Password Standard to require a minimum of 8 characters and enable complexity. However the Novell Netware password configuration settings do not match the revised Standard.

OIAI reviewed password restrictions for Novell Netware and determined that complexity which requires a combination of numeric, upper case, lower case, and special characters cannot be enabled. The Novell Netware password configuration settings are currently set to require a minimum of six characters, forced password changes every 90 days, unique passwords, and six grace logins.

Employees who are unaware of the Novell Netware Login Password Standard may not follow it and create passwords that are easily guessed.

RECOMMENDATION

DFAS/ISD should change the Novell Netware password configuration settings to better match the Novell Netware Login Password Standard and IT Governance Institute's best practice guidelines. We recommend the Novell Netware password configuration settings be changed:

- Minimum number of characters be increased from six to eight.
- Grace logins be reduced from six to three.

RESPONSE FROM DFAS/ISD

"Within the next three months, ISD will work with Internal Audit staff and the Technical Review Committee to finalize and implement the appropriate Netware password configuration settings."

4. DFAS/ISD SHOULD REVISE PASSWORD SETTINGS TO FOLLOW BEST PRACTICE GUIDELINES, WHEN CAPABLE.

DFAS/ISD implemented Recommendation No. 7, page 9, which was to ensure that user ID and password controls are in place for accessing City systems. This recommendation refines Recommendation No. 7, addressing password parameter or configuration settings for core systems.

The City's core systems all require a user ID and password to access. The password configuration settings, which control the format of passwords of some of these systems, are not as secure as they should be according to IT Governance Institute best practice guidance. Further refinement of these settings has not been performed by DFAS/ISD.

Password parameter settings should be configured to best practice guidance to further decrease the possibility of unauthorized access. The IT Governance Institute recommends the following guidelines:

- Minimum password length of 8 characters.
- Mix of numbers, upper & lower case letters, and special characters (referred to as complexity).
- Unique passwords (prohibit use of prior passwords).
- Passwords changed on a regular basis.
- Lockout after 3 to 5 attempts.
- Unauthorized attempts are recorded in audit logs.

Employees who are unaware of good password guidelines may not follow it and create passwords that are easily guessed or cracked.

Threats to data and systems have increased due to identity theft and access to the Internet, email, and web applications. DFAS/ISD has addressed these threats with firewall devices and network monitoring but further refinement of system password settings has not been performed. User ID and password protection is the first line of defense against unauthorized access.

RECOMMENDATION

DFAS/ISD should revise password settings for the following systems to better match IT Governance Institute's guidance. Suggestions include:

1. PeopleSoft CRM
   Help Desk and 311 systems
   a. Minimum number of characters = 8
   b. Enable complexity
   c. Maximum password age = 180 days
   d. Lockout after 3 attempts
   e. Prevent reuse of last 5 passwords

2. Active Directory
    a. Minimum number of characters = 8
    b. Enable complexity
    c. Minimum password age = 1 days
    d. Lockout after 3 attempts
    e. Prevent reuse of last 5 passwords

3. FileNet
    a. Enable complexity
    b. Prevent reuse of last 5 passwords

4. Lotus Notes
    a. Lockout after 3 attempts.
    b. Maximum password age = 180 days

I-Notes does not meet best practice guidelines but it is not used to process critical or sensitive transactions so it is not included in our recommendations. I-Notes stores telephone directory information and is used for TRC requests.

RESPONSE FROM DFAS/ISD

"Within the next three months, ISD will work with Internal Audit staff and the Technical Review Committee to finalize and implement the appropriate password configuration settings for the systems listed."

CONCLUSION

The CAO and DFAS/ISD have fully implemented or resolved six of the nine recommendations noted in the initial audit. Two recommendations were partially implemented. One recommendation was not implemented. Four additional findings were noted during this follow-up. The CAO and DFAS/ISD need to further strengthen procedures regarding termination procedures, user account management, and passwords.

We appreciate the assistance and cooperation of HRD and DFAS/ISD personnel during the follow-up.

Senior Information Systems Auditor

REVIEWED:

Audit Manager	Internal Auditor
APPROVED:	APPROVED FOR PUBLICATION:
Carmen Kavelman, CPA, CISA, CGAP Director Office of Internal Audit & Investigations	Chairperson, Accountability in Government Oversight Committee