MANAGEMENT AUDIT REPORT

OF

COMPUTER USER IDs

REPORT NO. 05-107

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

June 28, 2006

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico 87102

Audit: Computer User Ids
05-107

FINAL

INTRODUCTION

User Identities (Ids) and passwords are the simplest and most common form of computer user authentication. As technology progresses, individuals still make the same basic mistakes of choosing obvious passwords, writing passwords down, and sharing passwords. The number of passwords and other secret codes that individuals have to remember has increased dramatically. For example, an average person will have a user Id and password for online banking and online bill paying, access codes for voicemail and unlocking cell phones, secret codes for ATMs, passwords for logging into websites, security codes for offices, and a user id and password to access a computer at work. In the security world, there is continuing pressure to make networks more secure. Network security is diminished when passwords are easy to guess, written on paper, left in obvious places, and shared with others. Passwords are confidential information, and should not be shared with anyone.

The Office of Internal Audit and Investigations (OIAI) conducted an audit of the City of Albuquerque's Computer User Ids as part of the FY 2005 approved audit plan.

AUDIT OBJECTIVES

The objectives of our audit were to determine:

- Are passwords set to expire after a predefined interval?

- Does the Information Systems Division (ISD) deactivate user Ids after a predefined interval of non-use?
- Does the help desk require employees to provide information to positively identify them as account holders to have the password set for a User Id?
- Are all user Ids required to have passwords?
- Does the system automatically inhibit the use of a User Id after the standard number of access attempts with an incorrect password?
- Is intruder detection activated?
- Are there policies on logical security and access control?
- Does the system not permit the re-use of prior passwords for a minimum standard number of iterations?
- Does the system 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?
- Has a parameter been activated on the Novell network that requires passwords to be in a specified format of exactly 8 characters, no vowels, at least 1 number, at least 1 capital letter, and at least 1 special character?
- Do all City of Albuquerque (City) issued user Ids consist of 6 alphabetical characters with the 3 character prefix consisting of the user's department and the 3 character suffix consisting of the user's initials?
- Can ISD provide documentation of revoked user access? Does ISD maintain a file of user access revocation?
- Is a termination report sent to the Help Desk to deactivate user Ids for employees who are no longer employed by City?

SCOPE

Our audit did not include an examination of all aspects of the City Computer User Ids. Our audit test work was limited to user Ids and passwords Citywide for the period of December 1, 2005 thru December 31, 2005.

This report and its conclusions are based on information taken from a sample of transactions and do not purport to represent an examination of all related transactions and activities. A review of internal controls relating to Computer User Ids was made to assure management that City policies and regulations regarding Computer User Ids are being properly administered. The audit report is based on our examination of activities through the completion date of our fieldwork, and it does not reflect events after that date.

The audit was conducted in accordance with Government Auditing Standards, except Standard 3.49, requiring an external quality control review. The audit was also conducted in accordance with Control Objectives for Information and related Technology (COBIT) Audit Guidelines, of the IT Governance Institute. These guidelines enable the auditor to review specific Information

Technology (IT) processes against COBIT's recommended Control Objectives to help assure management where controls are sufficient. These guidelines also advise management where processes need to be improved.

METHODOLOGY

We conducted interviews with IT individuals by sending a survey to a judgmental sample of City departments. We compiled the survey results, and compared results to City IT policies and standards to determine compliance. We performed test work on audit objectives using statistically sampled user names. Fieldwork was conducted at City Hall and various City departments. A survey was sent to seven City departments judgmentally sampled based on size of IT functions to determine compliance with information technology policies and standards. Statistical samples were selected from the seven departments to perform test work on our audit objectives.

FINDINGS

The following findings concern areas that we believe could be improved by the implementation of the related recommendations.

1. CITY DEPARTMENTS SHOULD PROMPTLY NOTIFY ISD IN WRITING WHEN A DEPARTING EMPLOYEE'S COMPUTER ACCESS IS TERMINATED.

   Section 4c of the Employee Clearance Form, P-4, instructions state, "the supervisor should ensure the departing employee's computer access is terminated with a service request or an e-mail message to the ISD Help Desk."

   ISD management informed OIAI that the ISD helpdesk is not promptly notified when an employee terminates, transfers to another position in the City, or is found to be involved in serious inappropriate or illegal activities. The instructions of the P-4 only recommend that supervisors contact ISD to cancel employee computer access. There is no written instruction that requires department supervisors to contact ISD immediately to terminate departing employees' computer access.

   OIAI surveyed seven City departments regarding compliance with IT policies and standards. Two departments indicated that a formal procedure does not exist for removing employee computer access when the individual transfers to another department.

   OIAI tested a statistical sample of 63 terminated employees from the ISD Help Desk terminated employees report to determine if their computer user access was revoked in a timely manner. OIAI defined timely as less than seven days from the date the individual terminated employment with the City.

Our results revealed the following:

- Sixty-one employees' computer access was not revoked in a timely manner. The following categorizes the amount time taken to revoke the employees' access from the date of the employees termination:

Number of Employees	Termination Period
2	Greater than one year
2	Greater than 180 days up to one year
2	Greater than 120 up to 180 days
5	Sixty up to 120 days
35	Thirty but less than 60 days
15	Seven but less than 30 days

Four terminated employees, which are part of the sixty-three sampled, continue to have access to some City computer applications.

There is time lag between the date that the individual terminates employment, and when ISD Help Desk personnel receive notification to revoke computer access. If access for terminated employees' is not revoked immediately, prior employees and unauthorized individuals may gain access to City computer systems. ISD management informed OIAI that Help Desk personnel are never notified to cancel computer access to City systems when temporary employees, vendors, and contractors terminate services with the City.

If the ISD helpdesk is not promptly notified to terminate departing employees' computer access, these employees may gain unauthorized access to the City computer system.

COBIT – Recommends establishing procedures to ensure timely actions in relation to requesting, establishing, issuing, suspending and closing user accounts.

RECOMMENDATION

The CAO should ensure that a process and policy are developed requiring all City departments to promptly notify ISD in writing when a departing employee's computer access is terminated.

RESPONSE FROM THE CAO

"The CAO agrees that ISD should be promptly notified when a departing employee's computer access should be terminated. The CAO will work with the Human Resources Department to ensure that

departmental HR Coordinators are tasked with the responsibility to notify ISD whenever any employee is terminating or transferring."

2. INFORMATION TECHNOLOGY POLICIES AND STANDARDS SHOULD BE PERIODICALLY COMMUNICATED TO CITY EMPLOYEES.

The City Information Technology Policies and Standards regarding the User Id Security Policy state, "User Ids shall not be shared among users." They also state, "Unique User Ids of a standard format, with passwords, shall be required to access all multi-user computer systems." The Standard for Approved Exceptions to User Id Security Policy currently does not list any exceptions granted for the use of shared user Ids.

ISD management informed OIAI that they are aware that City employees share their user Ids and passwords with other employees and/or personnel not employed by the City. ISD management also informed OIAI that they aware of departments using generic user id accounts.

OIAI surveyed seven City departments regarding compliance with IT policies and standards and determined the following:

- Five stated that their employees share user Ids and that generic user Ids are in place.
- Three do not have procedures for removing computer access when an employee terminates employment or transfers to another department.
- One was not aware of the Information Technology policy regarding the sharing of user Ids and passwords.
- One follows its own policy that allows the use of generic user Ids on a restricted basis.

When generic or shared user Ids are used, it is impossible to track user access, trace unauthorized activity, and unauthorized individuals may gain access to the City systems.

RECOMMENDATION

The CAO should ensure that information technology policies and standards are periodically communicated to city employees.

RESPONSE FROM THE CAO

"The CAO agrees that information technology policies and standards should be periodically communicated to City employees. Information technology policies, standards and procedures are available on the City intranet, are reviewed and updated as necessary on a regular basis by the Information Systems Committee and discussed during regular IT User Group meetings.

"To reinforce this information sharing, beginning in August, 2006, every City technology user will be required to annually refresh their knowledge and awareness of IT policies and procedures by completing an annual information technology security certification process."

3. CITY EMPLOYEES SHOULD BE PERIODICALLY INFORMED ABOUT SAFEGUARDING COMPUTER SYSTEM PASSWORDS.

COBIT recommends that users should be initially and periodically asked to review rules and regulations for system access.

ISD management informed OIAI that they aware that City employees hide their computer system passwords in obvious locations where others may find them and obtain access to COA systems.

City department IT representatives have been informed about safeguarding computer system passwords through communications such as IT User Group meetings. City employees continue to store system passwords in obvious places. If employees do not safeguard the passwords, unauthorized individuals may gain access to City computer systems.

RECOMMENDATION

The CAO should ensure that City employees are periodically informed about safeguarding of computer system passwords. This could be done by creating a policy that requires employees to safeguard computer system passwords.

RESPONSE FROM THE CAO

"The CAO agrees that safeguarding of passwords is an important aspect of IT security policy. That is why the User Id Security Policy currently states "User Ids and passwords shall not be shared among users". The CAO notes that creating a policy does not, however, change behavior.

As long as employees are required to have multiple passwords to access multiple systems during their daily work, there will be a tendency to engage in behavior that may compromise the safeguarding of passwords. The CAO is hopeful that the annual information technology security certification process will make users more aware of this fundamental safeguard."

4. ISD SHOULD ALWAYS MONITOR AND INVESTIGATE UNSUCCESSFUL LOGINS.

ISD management informed OIAI that it does not monitor unsuccessful logins to City computer systems. ISD management also informed OIAI that there is not available staff within the City to monitor login activity.

The City Information Technology Policies and Standards regarding User Ids states, "Unsuccessful access attempts and access violations shall be automatically logged, reported, and reviewed by the System Administration function for appropriate follow-up."

If unsuccessful logins are not monitored, security violations may result.

RECOMMENDATION

ISD should always monitor and investigate unsuccessful logins.

RESPONSE FROM DFAS/ISD

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

5. CITY DEPARTMENTS REQUIRING SHARED/GENERIC COMPUTER USER IDS SHOULD FOLLOW THE CITY USER ID SECURITY POLICY EXCEPTIONS PROCEDURE.

The City Information Technology Policies and Standards – User Id Standard requires user Ids to consist of six alphabetic characters, combining a three-character prefix

identifying the user's department or function area and a three-character suffix comprising the initials of the user's name as listed in the records of the Human Resources Department.

OIAI tested 60 user Ids for compliance with the City User Id Standard. Five of the 60 sampled user Ids are not in compliance with this standard. These user Ids are generic Ids.

The Information Technology Policies and Standards – User Id Security Policy states, "User Ids and passwords shall not be shared among users."

If user Ids are not in compliance with the standard, it will be impossible to identify the actual user. If user Ids are generic, it will be impossible to track user access, and trace unauthorized activity.

One City department that is not in compliance has its own policy that allows for the use of generic Ids on a restricted basis. The other two departments have generic Ids set up for convenience purposes.

The City Information Technology Policies and Standards - User Security Policy Exception Procedure requires Departments that must use shared/generic user Ids to submit a written request with Department Director approval to the ISD Technical Review Committee (TRC).

RECOMMENDATION

The CAO should require that all departments needing to establish shared/generic user Ids to follow the City User Id Security Policy Exceptions Procedure.

RESPONSE FROM CAO

"The CAO agrees that departments needing shared/generic user Ids for valid business purposes should comply with the appropriate information technology policies, standards and procedures.

"All departments identified as having shared/generic user Ids were notified on June 15, 2006 of: 1) their deviation from policy, standard and procedure; 2) referred to the policy, standard and procedure governing this issue; 3) advised to immediately begin the process to obtain the waiver; and 4) advised that all generic user Ids will be automatically invalidated on a specific date unless the department had taken affirmative action to retain the use of shared/generic user Ids."

6. DFAS/ISD SHOULD ENFORCE THE PASSWORD STANDARD FOR THE NOVELL NETWORK.

The City Information Technology Novell Login Passwords Standard requires passwords to be in a specified format. The specified format is:

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

ISD personnel informed OIAI that the parameter has not been activated on the Novell network that requires passwords to be in the specified format.

ISD determined in Fiscal Year 2003 that the module to activate the password parameter would cost approximately $120,000. ISD presented this potential procurement to the TRC and Information Systems Council (ISC). Due to the expense, ISC decided to configure Novell to allow only three attempts with an invalid password. ISC and ISD view the configuration as a compensating control as opposed to purchasing the module.

ISD will not be able to enforce the Novell Login Passwords Standard unless the password parameter module is purchased.

The 2003 Miller IT Audits guide discusses that the rules of password structure or syntax require at least eight characters and enforce a combination of alpha and numeric characters.

RECOMMENDATION

ISD should change the Novell password standard to comply with the rules discussed in the 2003 Miller IT Audits guide.

RESPONSE FROM DFAS/ISD

"ISD agrees with the recommendation. ISD will 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."

7. USER ID AND PASSWORD CONTROLS SHOULD BE IN PLACE FOR ACCESSING CITY SYSTEMS.

The City Information Technology Policies and Standards – User Id Security Policy states,

> A standard shall be published detailing specifications for passwords, including…expiration intervals. A system shall automatically inhibit the use of a User Id after a standard number of access attempts with an incorrect password. A system shall not permit the re-use of prior passwords for a minimum standard number of iterations. A system shall automatically terminate a user session after a minimum standard period of inactivity. A system 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."

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

- Passwords are set to expire after a predefined interval.
- Passwords are set to deactivate after a predefined interval of non-use.
- There are a standard number of access attempts for incorrect passwords.
- The system requires a minimum number of iterations before permitting the re-use of prior passwords.
- The system generated a log of system transactions, and verified if the log provides the following transactions:

    - User who initiated the transaction
    - Date and time of the transaction
    - Type of entry
    - Data accessed or altered

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

- Four do not have the password set to expire at a predefined interval.
- Five do not have the user Ids set to deactivate after a predefined interval of non-use.
- Four are set to inhibit the use of a user Id after a standard number of access attempts with an incorrect password.
- Three do not limit the re-use of prior passwords for a standard number of iterations.
- Three do not provide an audit trail of transactions.

Security violations may result, if user Ids and passwords are not secure.

RECOMMENDATION

DFAS/ISD management should ensure that user Id and password controls are in place for accessing City systems.

RESPONSE FROM DFAS/ISD

"ISD agrees with the recommendation. While some systems are incapable of enforcing all rules, ISD will investigate options to synchronize passwords and enforce common password control attributes."

8. THERE SHOULD BE SEGREGATION OF DUTIES BETWEEN SYSTEM ADMINISTRATION AND SECURITY FUNCTIONS FOR ALL CITY COMPUTER SYSTEMS.

COBIT recommends enforcing segregation of duties to help avoid the subversion of critical processes by a single individual.

OIAI inquired about and observed the duties of Security and System Administrator for eight City computer systems (systems). OIAI determined that Security and System Administrative functions are not segregated for four systems.

According to ISD Management, the lack of segregation of duties is due to budgetary constraints which prevent IDS from hiring additional staff.

RECOMMENDATION

DFAS/ISD management should ensure that there is segregation of duties between System Administration and Security functions for all City computer systems. Since budgetary constraints exist, this could be accomplished by cross training individuals from different areas within ISD to serve in security roles for systems that currently have a lack of segregation of duties.

RESPONSE FROM DFAS/ISD

"ISD agrees in principle with the recommendation. Major line of business applications, such as finance, payroll, the new PeopleSoft billing (CIS) and constituent management (CRM) systems, have clear separation between system administration and application security functions. In addition, the Domino email security administrators are separated from the Unix system administrators. However, this approach

is not practical when the underlying system and the service offered are one in the same, such as Netware or Windows file sharing. However, ISD will continue to split the responsibilities where it is prudent to do so."

9. HELP DESK PERSONNEL SHOULD POSITIVELY IDENTIFY EVERYONE WHO REQUESTS THEIR COMPUTER SYSTEM PASSWORD TO BE RESET.

ISD requires all help desk personnel to positively identify all individuals requesting the reset of their computer systems passwords. Help desk personnel positively identify the individuals by requesting one of the following:

- Last four digits of their Social Security number
- Mother's maiden name
- Favorite color

The positive identification requirement is only verbal. There is not a formal written policy, procedure, or standard to enforce this requirement.

OIAI judgmentally selected a sample of fifteen City employees (employees) to contact the ISD help desk and request the reset of their computer system passwords. Two employees sampled had their passwords reset, but were not positively identified.

If employees requesting password resets are not positively identified, unauthorized individuals might be able to gain access to City computer systems.

RECOMMENDATION

DFAS/ISD management should ensure that all Help Desk representatives positively identify everyone who requests their computer system password to be reset.

DFAS/ISD management should formalize the positive identification requirement as part of the Information and Technology Policies and Standards.

RESPONSE FROM DFAS/ISD

"ISD agrees with the recommendation. We will stress to the Help Desk staff the importance of and the established requirement for validating an individual's identity before resetting passwords."

Other Items for discussion

For the long-term, ISD should consider using biometrics as a user identification technique.

Wikipedia, an international Web-based free-content encyclopedia, defines biometric authentication as follows: "In information technology, *biometric authentication* refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. Voice is considered a mix of both physical and behavioral characteristics, but all biometric traits share physical and behavioral aspects."

Usage of biometrics for authentication on a computer system is more accurate than a password. This is due to biometrics linking an event to a particular individual whereas a password can be used by someone other than the authorized user. Biometric technology will enable the City to better protect computer systems as well as IT assets from being accessed by unauthorized individuals.

CONCLUSION

City systems are at risk since User Ids and Passwords are not always secure. Risk to City systems can be mitigated by ensuring departments follow City Policies regarding user IDs and passwords. Developing policies and procedures when they do not exist regarding user Ids and passwords with ISC's endorsement will enhance the existing system of controls.

We appreciate the cooperation of the DFAS/ISD staff during the audit.

_____
Senior Information Systems Auditor

REVIEWED:

_____
Audit Supervisor

APPROVED:

_____
Carmen Kavelman, CPA, CISA, CGAP
Director
Office of Internal Audit & Investigations

APPROVED FOR PUBLICATION:

_____
Chairperson, Accountability in Government
Oversight Committee