FINAL

MANAGEMENT AUDIT REPORT

OF

DEPARTMENT OF FINANCE AND ADMINISTRATIVE SERVICES

INFORMATION SERVICES DIVISION

REMOTE ACCESS TO CITY COMPUTERS

REPORT NO. 02-103

CITY OF ALBUQUERUQE
OFFICE OF INTERNAL AUDIT

Internal Audit

City of Albuquerque

P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

July 17, 2003

Internal Audit Committee
City of Albuquerque
Albuquerque, New Mexico

Audit: Department of Finance and Administrative Services
Information Services Division
Remote Access to City Computers
02-103

FINAL

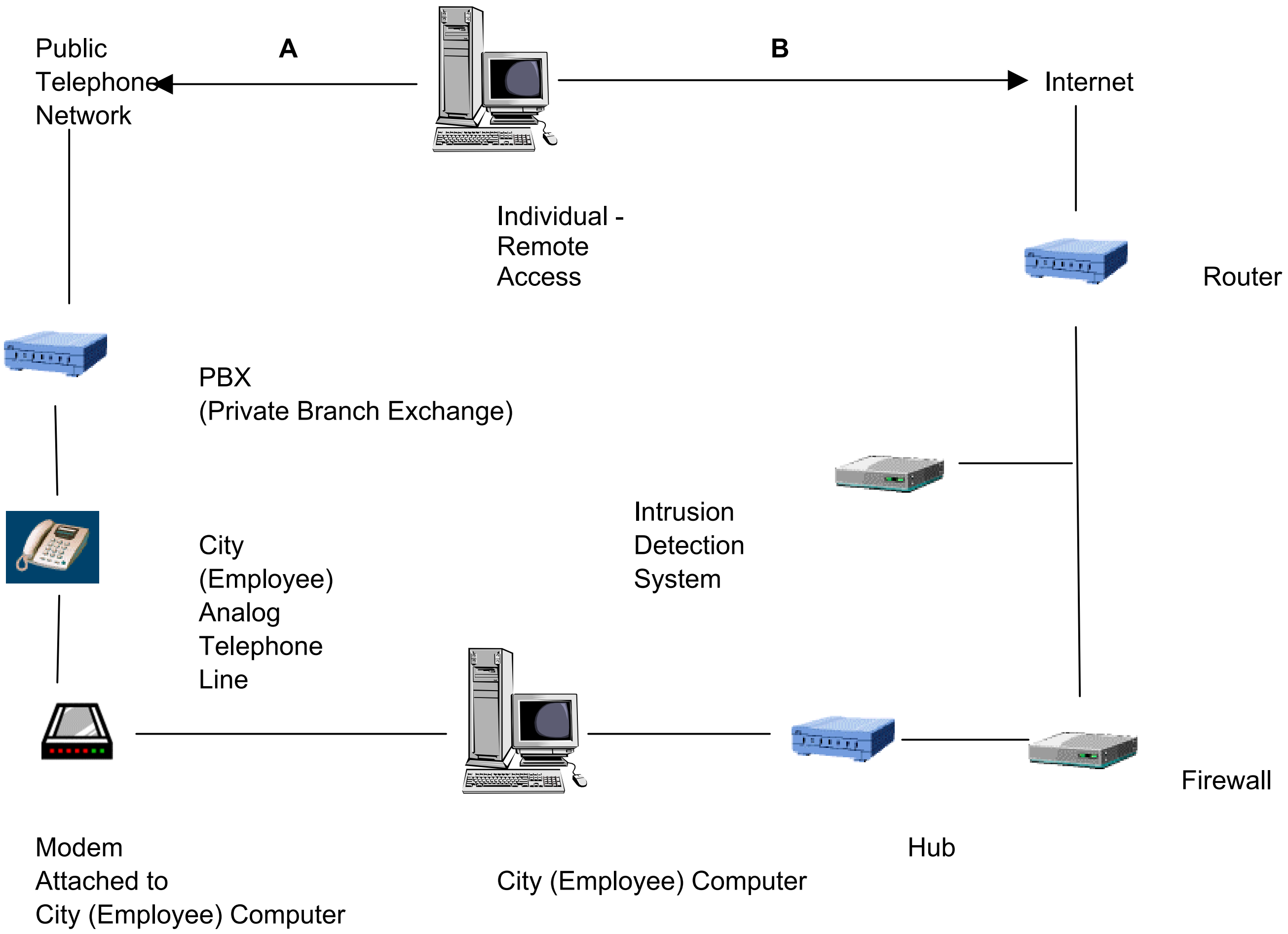
INTRODUCTION

The Office of Internal Audit performed a management audit of the Department of Finance and Administrative Services (DFAS), Information Systems Division (ISD), Remote Access to City Computers. The audit was included in the FY02 Audit Plan. Included in this audit was a determination of who has remote access to City computers as well as a review of the internal control environment and operational policies and procedures for remote access.

Remote access is the ability to connect and gain access to internal network resources that are physically disbursed. Usually, this means that a workstation (computer) equipped with remote access software will give authorized users at remote sites (such as their homes) dial in access over a phone, using a modem, or dial-up digital service over the Public Telephone Network. This enables users to troubleshoot problems, read E-mail, run applications, and transfer files to and from organization computers. A modem is a device that converts signals from one form to a form compatible with another kind of equipment.

Remote access devices, in conjunction with the Public Telephone Network, can cause a security risk to City government. Figure 1, below, shows an example of an individual attempting to gain remote access to the City of Albuquerque network. If this individual accesses the network via path A, he/she bypasses the firewall, and might be able to access secure areas within the City's network even though this individual might not have proper authorization. A firewall is a device that forms a barrier between a secure and an open environment. Moreover, a firewall acts as a system or combination of systems that enforces a boundary between two or more networks. The internet is an example of an open environment. It is much more secure for the individual, in the example discussed above, to access the City's network using path B (see figure 1). Furthermore, the individual will not be able to pass through the firewall unless he/she has authorization, such as a password.

Figure 1



The potential security risks of having modems attached to individual employee computers within the City are as follows:

- Unauthorized external access to internal networks or computer systems
- Unauthorized internal access to external networks or computer systems
- Loss of software configuration control

The most significant of the above potential security risks is the possible access by outsiders to the City's internal network. A firewall may block access from the Internet, but the presence of a modem absolutely bypasses this safeguard. A modem essentially places an unlocked backdoor in the security boundary that had been designed to protect the internal network. Another risk is associated with authorized users performing unauthorized activities from the internal network. Devices are protected by required logins and the routers and switches have encrypted passwords unreadable even when you are attached to the devices. However, knowledgeable individuals can capture information and then be able to login to a device to retrieve or corrupt that information.

SCOPE

Our audit did not include an examination of all the functions, transactions, and activities related to remote access to city computers. Our audit test work was limited to the following areas:

- Policies, Regulations, and Issues
- Controls/Securities and Risks
- Known and Unknown Users and Vendors with remote access

The audit was conducted in accordance with Government Auditing Standards, except Standard 3.33, which requires an external quality control review.

FINDINGS

The purpose of an internal audit is to identify changes in the auditee's activities which would improve its effectiveness, efficiency and compliance with administrative policies and applicable rules and regulations. Therefore, the auditee's activities which appear to be functioning well are not usually commented on in audit reports. The following findings concern areas that we believe could be improved by the implementation of the related recommendations.

1. DFAS MANAGEMENT SHOULD CONSULT WITH THE INFORMATION SYSTEMS COMMITTEE TO ESTABLISH AND IMPLEMENT CONTROLS OVER UNAUTHORIZED MODEM USAGE BY CITY EMPLOYEES.

We inquired with ISD management about what controls are in place over unauthorized modem use by city employees. ISD management indicated that no controls have been established for unauthorized modem usage.

A modem provides a quick, easy, and inexpensive means to circumvent the security features of the network. A firewall is in place to block access by outsiders (from the

Internet) to an entity's internal network, the use of a modem completely bypasses this security safeguard. Another risk when a modem is present is that employees have the ability to download software from other sites, bypassing the normal security safeguards ISD has in place, and installing potentially dangerous software on the system. This increases the potential of a virus being introduced into the systems connected to the internal network.

Good network security practices include establishing and implementing controls over vulnerable areas. It is essential to maintain proper authorization control of modems within the City.

RECOMMENDATION

The Information Services Division should prepare an Administrative Instruction to establish controls for modem use by City employees. The Administrative Instruction should be presented to the Technical Review Committee (TRC) and the Information Systems Committee (ISC) for approval. These controls could include but not be limited to the following:

1. Policies, procedures, and guidelines regarding employee modem usage.

2. A telephone firewall to protect data networks by securing telephone networks. It can serve as a barrier to intruders, and prevent them from accessing the organization's internal network. Furthermore, it can restrict data communication to specific telephone lines identified by the security policy as allowing modem or fax connections. In addition it can block all incoming or outgoing data communication on telephones authorized as voice only.

3. A telephone intrusion detection system to monitor the telephone system and alert the telephone administrator when an unauthorized act occurs. The administrator can then take the appropriate action whether that is deemed to be termination, monitoring, or redirection of the connection.

4. ISD management should consider obtaining a war dialer, and running it against the telephone lines to determine where unauthorized modems are in use. The unauthorized modems can then be removed.

ISD Management should also consider periodically running the war dialer so new unauthorized modems can be detected as quickly as possible.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs. ISD will submit appropriate documentation to the TRC and ISC for approval. The suggestion of an Administrative Instruction, based on this documentation, and this audit will be addressed to the ISC."

2. DFAS MANAGEMENT SHOULD COMMUNICATE ITS POLICY REGARDING REMOTE ACCESS TO THE CITY'S NETWORK.

During our fieldwork, ISD management stated that only three City employees have been authorized to have remote access to the City network via an external modem. However, the City does not have a written policy that communicates the requirements for remote access to City systems.

We e-mailed the management of all other City departments and asked if any of their employees have remote access to the network. We determined the following from our inquiry:

- Eight City employees that have not been authorized by ISD have the ability to access the City network remotely using an external modem and remote access software.

- Two City employees do not yet have remote access capability, but are in the process of obtaining such access using the same method as mentioned above.

- There could be other employees using software whose managers are unaware of this capability.

During our fieldwork, we also observed that a vendor representative, who works on-site exclusively for the City, has a workstation, with access to the City network. This workstation also has an external modem attached to it, and uses remote access software. This workstation as well as the external modem is left on 24 hours a day.

Our test work also consisted of using a war dialer to detect external devices, such as modems attached to analog telephone lines. Our war dialer detected sixty-three analog lines with devices attached to them.

- We were unable to locate twelve of the sixty-three analog lines.

- Five of the sixty-three analog lines were labeled incorrectly.

- Five of the sixty-three analog lines have modems attached to them.

- Four of the five modems are being used in conjunction with remote access software. The other 58 devices included facsimile machines and monitoring devices.

- One analog line is being charged to the wrong activity number.

The potential security risks of having modems attached to individual employee computers within the City are as follows:

- Unauthorized individuals from outside of the City might be able to gain access to internal networks or computer systems.

- Authorized users, such as service personnel, contractors, or consultants may be given temporary access to the system, which may permit them to access external systems and transmit confidential information from the internal network.

- City employees might be able to download software from other sites, circumventing security safeguards that ISD has in place, and install potentially dangerous software on their workstations, and possibly introduce viruses to the internal network.

A modem essentially places an unlocked backdoor in the security boundary that had been designed to protect the internal network.

Only three employees within the City have been authorized to use an external modem for remote access, although other employees have independently connected remote access devices to their City computers. One reason may be that the City has not established and communicated a formal policy related to remote access.

RECOMMENDATION

DFAS-ISD management should prepare a formal written policy regarding remote access to the City's network. In addition, ISD management should develop an administrative instruction for consideration by the CAO. The administrative instruction could require that ISD authorize all purchases of remote access software including the version level of the software that has the appropriate controls, such as a user name and password.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs. ISD will submit appropriate documentation to the TRC and ISC for approval. The suggestion of an Administrative Instruction, based on this documentation, and this audit will be addressed to the ISC."

3. DFAS MANAGEMENT SHOULD ACTIVATE THE OPTION IN STARGAZER TO PROMPT USERS TO CHANGE THEIR PASSWORDS ON A REGULAR BASIS.

Stargazer is software set up on a server in ISD that enables City employees to remotely access various City computer applications via the Internet. Many applications can be accessed remotely using Stargazer.

ISD management considers the Stargazer connection to be an authorized method of remote access to city applications. The user must enter a user identification and password. Users are not currently required to change their passwords, but Stargazer does offer the option to prompt users to change their passwords. ISD management has chosen not to activate this option. If passwords are not changed on a regular basis (i.e. every 30 to 60 days), an unauthorized person might guess a password, and repeatedly gain access to various city applications.

RECOMMENDATION

DFAS-ISD management should activate the option in Stargazer to prompt users to change their passwords on a regular basis.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs. This has been implemented. Users of Stargazer are now required to change their password every 45 days."

4. THE CULTURAL SERVICES DEPARTMENT SHOULD ENSURE THAT AQUARIUM SYSTEM PASSWORDS ARE CHANGED REGULARLY, AND THAT SYSTEM SECURITY IS MAINTAINED.

As part of our fieldwork, we used a war dialer to help us detect possible external modems in use at the City. While performing our test work, we identified three modems in use at the Aquarium. We determined that two of the modems, in conjunction with software, enable individuals to remotely dial in to the corresponding systems from offsite locations. The third modem is attached to a monitor system that dials out to specific pagers when problems occur. Aquarists carry the pagers. One of the aquarists must physically return to the building to deal with the problem.

One of the systems that can be remotely accessed with one of the modems mentioned above requires a password. This system is used to monitor heating and cooling at the Aquarium. It also controls the opening and closing of doors and windows at the greenhouse. At the time of our audit fieldwork, the system password was not changed on a regular basis (i.e. every 30 to 60 days). Since this password was not changed on a regular basis the greenhouse was susceptible to damage or theft. For example, a former employee who was disgruntled might be able to gain access to the green house, and cause damage.

The other system, known as the "Life Support computer," controls and monitors all filters, circulation pumps, heat exchangers, make-up (add or subtract), and the ozone system of various displays. These displays include the sharks, coral reef, large fish, eels, bat ray, tide pool, and water recovery system. Aquarium management estimates the livestock in these displays to be worth approximately $200,000. The operations manager is able to remotely access this system from his home. A password must be entered in order to access this system. At the time of our audit fieldwork, this password was not changed on a regular basis (i.e. every 30 to 60 days). Additionally, the passwords are only three digits long. The system generates an access log that actually shows the three-digit password. During our test-work we noted that an operator was not always present when the system was signed on. Furthermore, the door to the room that contains the Life Support system is always left open. It might be possible for an unauthorized person to get the password from the activity log, and access the Life Support system from somewhere offsite. The operations manager estimates the Life Support equipment to be worth approximately $3.5 million. Since the room was not always secure this equipment was subject to theft, and could be a significant loss to the City.

RECOMMENDATION

The Cultural Services Department (CSD) should ensure that aquarium system passwords are changed regularly (i.e. every 30 to 60 days), and that both system and physical security are maintained at all times.

EXECUTIVE RESPONSE FROM CSD

"CSD concurs. Effective immediately, all aquarium staff will ensure that the doors remain locked and the control room locks will be rekeyed to restrict access to authorized personnel only. In addition, the aquarium system passwords will be changed every 30 days, effective August 15, 2003. These changes will ensure both system and physical security."

5. DFAS MANAGEMENT SHOULD RESTRICT ACCESS TO THE LIST OF ANALOG TELEPHONE NUMBERS.

Analog telephone lines are data capable lines. They enable computers to communicate with each other. A hacker can use analog telephone lines in conjunction with a war dialer to locate external modems attached to individual computers within an organization.

During our fieldwork, we asked ISD management to identify individuals who have access to the list of City analog telephone numbers. We were told that there has never been an instruction indicating that these telephone numbers should be confidential. Therefore, this information is public, and anyone who requests this list may have access to it. If the list of City analog telephone numbers is not kept confidential, unauthorized individuals might be able to use this information in conjunction with a war dialer to gain access to the City network, or other systems/servers and cause damage to sensitive information.

Chapter 14 Article 2 of the New Mexico State Statutes – Inspection of Public Records, 14-2-1 – Right to inspect public records; exceptions, states, "Every person has a right to inspect any public records of this state except . . .as otherwise provided by law."

According to an Assistant City Attorney, determining whether access should be granted to the list of analog telephone numbers should depend on the nature of the request. If ISD receives a request for the list of analog telephone numbers the request should be forwarded to the City's Legal Department for review. Further, the requestor(s) should be informed that the request requires review by the Legal Department before a decision can be made whether or not access will be granted to the requested information.

RECOMMENDATION

DFAS-ISD management should consult with the Legal Department concerning restriction of access to the list of analog telephone numbers.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs. This has been implemented. ISD has met with the Legal Department, and the release of the City's analog telephone numbers list will be determined by Legal on a case-by-case basis, based on the requestor, purpose, etc."

6. DFAS SHOULD DEVELOP AN ADMINISTRATIVE INSTRUCTION THAT REQUIRES ALL DEPARTMENTS TO PERIODICALLY PERFORM A PHYSICAL INVENTORY OF TELEPHONE LINES.

There is not a current inventory list of all active telephone extensions for each department within the City. A review of the telephone listings sent to us from the City's telephone vendor indicated that some of the descriptions are either incorrect or have never been updated. We asked vendor representatives for a current listing. We were told that a current listing is not available. ISD management told us that they do not have the staff level necessary to perform physical inventories of active telephone extensions. Instead, ISD management performs an annual port (telephone line) inventory by sending an inventory listing to each department. Each department is responsible for verifying their own ports, and returning the list to ISD. The practice does not appear to provide complete results.

If the list of active telephone lines is not kept current for each department within the City of Albuquerque, it is difficult for management to determine if any active lines are not in use. In addition, the City might be paying for telephone lines that are not regularly or ever used. For example, we identified five active City telephone lines at a facility that is not being used. The building has signs indicating that it is for sale. The City is paying for these telephone lines. Additionally, anyone with access to the building could use the telephone lines for long distance calls that would be charged to the City.

RECOMMENDATION

DFAS-ISD management should develop an administrative instruction to be considered by the CAO that requires all departments to periodically perform a physical inventory of all telephone lines within their departments. This will enable individual department management to determine if there are telephone lines within their departments that are not regularly or ever used. Active telephone lines that are not regularly used should be eliminated.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs, but Telecommunication Services believes many departments do not have the necessary expertise or staffing to perform line audits. The City will attempt to develop a process, possibly in conjunction with budget development, to monitor the number of lines needed and used."

7. OTHER ISSUES IDENTIFIED DURING THE AUDIT

Although not directly related to the scope of the audit, we identified the following issues that could have an impact on the City's efficient operation.

A. DFAS MANAGEMENT SHOULD ENSURE ADEQUATE BACKUP FOR POSITIONS THAT PERFORM SENSITIVE FUNCTIONS.

The production control group is currently not staffed. ISD is using people from other areas to perform the essential functions of this group. The production control group is responsible for scheduling, monitoring, and running application software for the City's major production systems (e.g. Accounting and Utility Billing). Production control group employees also support the application system change control process by managing the transition of software between development, test and production environments. The production control group is responsible for isolating and resolving production application system problems on a 24-hour basis and implementing and enforcing security policies related to computer platform and application system access.

We determined that because of the staffing shortages, the applications programmers are currently moving their own work from the test environment to the production environment. Application programmers create programs that eventually run in the production environment. If these programs are not monitored by production control, the programmers may develop programs that cause damage and possibly fraud. For example, a programmer working with the source code for the payroll system might develop a program that allocates a small amount from every employees' pay check each pay period, and transfer the amount to a separate bank account set up by the programmer. Segregating the applications programming and production controls minimizes the possibility of such an occurrence.

In addition, the City has paid information system contractors to perform projects since no one else in the respective departments has the knowledge or skill to perform this type of work. During our fieldwork, we found contracts with two former City employees to work on systems. These employees were hired on contract because replacement personnel had not been trained on the systems.

It would be more efficient if City information system functions were adequately staffed. The City could avoid spending money on contractors. Good internal controls ensure that adequate backup is available for the positions that perform sensitive functions.

RECOMMENDATION

DFAS Management should have adequate backup for positions that perform sensitive functions. DFAS should address the staffing issue of the production control group as soon as possible.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs and, in the future, will ensure that cross training and backups are in place for positions that support the City's mission-critical systems. This assumes that budget is available and the required skill-sets can be hired."

B. ISD SHOULD PARTICIPATE IN INTERVIEWS OF CANDIDATES FOR POSITIONS IN OTHER DEPARTMENTS THAT REQUIRE INFORMATION SYSTEMS KNOWLEDGE AND SKILLS.

During our fieldwork we were informed that many departments within the City have non-qualified people working in technical/information system positions. Directors and managers responsible for hiring people for these positions come from non-technical backgrounds, and lack the knowledge to properly assess the individuals who apply for the positions. If directors and/or managers lack the technical knowledge to assess applicants, individuals may be hired or promoted into technical positions for which they are not qualified. It is important that an organization's hiring practices ensure that the most qualified employees are chosen to fill positions that require technical knowledge and abilities relating to information systems.

RECOMMENDATION

DFAS management should develop an administrative instruction, to be considered by the CAO, which requires all departments to include representatives from ISD when candidates are interviewed for positions that require information systems knowledge and skills in departments other than ISD.

EXECUTIVE RESPONSE FROM DFAS

"This has been implemented. The CAO issued a memo on June 16, 2003, to all departments requiring DFAS/ISD participation in all information systems position interviews."

CONCLUSION

By implementing these recommendations, the Department of Finance and Administrative Services, Information Services Division will more effectively and efficiently administer remote access to City computers.

We appreciate the assistance and cooperation of the personnel of DFAS-ISD and the other City departments and divisions involved in this audit.

____
Senior Information Systems Auditor

REVIEWED and APPROVED:

____
Debra D. Yoshimura, CPA, CIA, CGAP
Internal Audit Officer

APPROVED FOR PUBLICATION:

____
Chairman, Audit Committee