City of Albuquerque

Interoffice Memorandum **October 26, 2005**

Ref. No.: 05-02-103F

To: **Sandy Doyle, Director, Financial and Administrative Services Department**

From: **Carmen Kavelman, Acting Director, Office of Internal Audit**

Subject: **FOLLOW-UP OF MANAGEMENT AUDIT REPORT NO. 02-103, DEPARTMENT OF FINANCE AND ADMINISTRATIVE SERVICES, INFORMATION SYSTEMS DIVISION, REMOTE ACCESS TO CITY COMPUTERS**

Internal Audit performed a Follow-up Review of Management Audit No. 02-103, Department of Finance and Administrative Services, Information Systems Division, Remote Access to City Computers, dated July 23, 2003. The purpose of our review was to determine if the audit recommendations had been implemented.

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.

We determined the following:

RECOMMENDATION NO. 1

We recommended that the Information Services Division prepare an Administrative Instruction to establish controls for modem use by City employees. The Administrative Instruction should be presented to the Technical Review Committee, and the Information Systems Committee for approval.

The use of a modem can completely bypass the security safeguard of a firewall. A firewall is used to block access to the network by outsiders using the Internet. We determined that ISD management did not have controls in place for unauthorized modem usage. A modem provides a quick, easy, and

inexpensive means to circumvent the security features of a network. This increases the potential of viruses being introduced into the systems connected to the internal network.

ACTION TAKEN

The audit recommendation has been fully implemented. DFAS-ISD created a policy as part of the Information Technology Policies and Standards that disallows the use of a modem with City network assets unless it has been approved in advance and is then registered with the Technical Review Committee.

RECOMMENDATION NO. 2

We recommended that DFAS-ISD management prepare a formal written policy regarding remote access to the City's network.

We determined, through inquiry the following:

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

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

- There could be other employees within the City using access software and modems whose managers were unaware of this capability.

We also observed a vendor, who worked on-site exclusively for the City, who had a workstation with access to the City network. The workstation had an external modem attached to it, and used remote access software. Both were left on 24 hours a day.

We used a war dialer to detect external devices, such as modems attached to analog telephone lines. We detected four analog lines with modems attached to them, and were being used in conjunction with remote access software.

DFAS-ISD management told us that only three City employees were authorized to have remote access to the City network via an external modem. Management also told us that they did not have a written policy to communicate requirements for remote access to City systems.

ACTION TAKEN

The audit recommendation has been fully implemented. DFAS-ISD created a policy as part of the Information Technology Policies and Standards that disallows the use of remote connectivity software to connect to the City's network in any way unless approved in advance and then registered with the Technical Review Committee.

We re-tested the four analog lines (lines) with modems attached to them. Two of the four lines still have modems attached, and are used in conjunction with remote access software. One of the lines is still active but not in use.

The City of Albuquerque Information Technology Policies and Standards regarding Network Access/Connectivity states, "No remote connectivity software (i.e. PC Anywhere, Procomm, etc.) will be used to connect to the City's network in any way unless approved in advance and then registered with the Technical Review Committee (TRC). No modem will be used to connect to City network assets unless approved in advance and then registered with the TRC."

RECOMMENDATION

DFAS-ISD management should inform the users that are using modems to remotely access their computers that they are in violation of the ISD Network Access/Connectivity. These users should be offered an alternative means of remote access such as Virtual Private Network. Virtual private networks are secured private network connections, built on top of publicly-accessible infrastructure, such as the Internet or the public telephone network.

DFAS-ISD management should request the user with the active analog line to deactivate the connection.

EXECUTIVE RESPONSE FROM DFAS

"DFAS concurs. At the next monthly IT Users Group meeting, ISD will discuss the requirements of the Network Access/Connectivity policy. It is the responsibility of IT Users Group members to make their Department management aware of the policy. As with most City policies, it is the responsibility of department managers to ensure that their employees and contractors abide by this policy.

"In addition, DFAS will prepare a brief memo for distribution to Department directors reminding them of the importance of compliance with this policy."

RECOMMENDATION NO. 3

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

We determined that employees who remotely accessed the City network using Stargazer were never required to change their passwords. Stargazer offered the option to prompt users to change their passwords, but ISD management had chosen not to activate this option.

ACTION TAKEN

The audit recommendation has been fully implemented. DFAS-ISD management activated the age by date rules in Stargazer to notify the user every 45 days to change his/her password. In addition, there is warning and grace period of 5 days.

RECOMMENDATION NO. 4

We recommended that the Cultural Services Department (CSD) ensure that aquarium system passwords are changed regularly every 30 to 60 days and that both system and physical security are maintained at all times.

We determined that password for the heating and cooling system was not changed on a regular basis. The system also controlled the opening and closing of doors and windows at the greenhouse. The greenhouse was susceptible to theft since this password was not changed on a regular basis. We also determined that the password for the Life Support system (LS) was not changed on a regular basis. In addition, an operator was not always present when the LS system was signed on. The door to the room containing the LS system was always left open. Since passwords were not changed regularly and the room was not secure, it was possible for an unauthorized person to get access to the LS system, and the equipment worth approximately $3.5 million was subject to theft.

ACTION TAKEN

The audit recommendation relating to the heating and cooling (HVAC) system has been fully implemented. The HVAC system has been moved to a secure area, and passwords are changed every 30 to 60 days.

The audit recommendation relating to the LS system has been partially implemented. The door to the room containing the LS system is always locked. The LS system in no longer remotely accessed. The modem has been removed. The administrative password to the LS system is not

changed on a regular basis. Internal Audit and Aquarium personnel verified that the password is a permanent part of the LS system and cannot be changed.

FOLLOW-UP RECOMMENDATION

CSD should ensure that future systems allow passwords to be changed.

EXECUTIVE RESPONSE FROM CSD

"CSD concurs. The LS system in place at the aquarium at the time of the original audit and the follow-up did not allow the password to be changed. Two weeks ago, the system at the aquarium was upgraded. Cognizant of the concern about the inability to change the password, CSD requested that the upgraded system allow for the password to be changed on a regular basis. That capability exists in the upgraded system."

RECOMMENDATION NO. 5

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

We determined that the analog telephone number list was not confidential, and that it was considered public information. We informed DFAS-ISD management that if this list was not kept confidential, unauthorized individuals could use this information to gain access to the City network, or other systems/servers and cause damage to sensitive information.

ACTION TAKEN

The audit recommendations have been partially implemented. We were told by DFAS-ISD management that DFAS-ISD and the Legal department (Legal) held a meeting, and decided that the release of the City's analog list will be determined by Legal on a case-by-case basis. However, DFAS-ISD was unable to provide information such as memos or minutes documenting this decision. Since this information was not available, the Auditor was unable to verify if the initial recommendation had been addressed.

FOLLOW-UP RECOMMENDATION

DFAS-ISD should ensure that documentation such as memos or minutes is maintained when consulting the Legal department on issues, such as who should have access to the analog telephone number listing.

EXECUTIVE RESPONSE FROM DFAS

"Any requests for the City's list of analog lines would, of necessity, have to be routed to or through ISD's Telecommunications group because they maintain the list of analog lines. Based on their conversations with the Legal Department, the Telecommunications group will forward any such request to the Legal Department for their written determination."

RECOMMENDATION NO. 6

We recommended that DFAS-ISD management 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.

We determined that there was not a current inventory list of all active telephone extensions for each department within the City. We were told by ISD management that they did not have the staff level necessary to perform physical inventories of active telephone extensions. Instead, an inventory is performed on an annual basis. If the list of active telephone lines is not kept current for each department within the City of Albuquerque, it would be difficult for management to determine if any active lines were not in use. We identified five active lines at a vacant City building. The City was still paying for these lines. Anyone with access to this building could have used the telephone lines for long distance calls that would be charged to the City.

ACTION TAKEN

The audit recommendation has been partially implemented. DFAS-ISD management did not develop an Administrative Instruction to be considered by the CAO. Departments are not periodically performing physical inventories of their telephone lines. ISD Telecommunications has an active telephone lines list that is available to all City departments upon request. This list was revised after the remote access audit was issued. This list is updated on an ongoing basis each time a change is made to the analog telephone line system.

FOLLOW-UP RECOMMENDATION

DFAS-ISD should send the list to all City departments for verification quarterly. ISD should develop a policy for approval by the CAO that requires City departments to inventory their telephone lines upon receipt of the analog telephone list.

EXECUTIVE RESPONSE FROM DFAS

"At a minimum, during the annual budget process, Departments are expected to verify the analog lines they will pay for and notify ISD of lines that should be removed. Since analog line costs are a small portion of each Department's annual budget, it is not cost effective to require an inventory be done more often than annually."

RECOMMENDATION NO. 7

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

We determined that the production control group was not staffed, and that employees from other ISD areas were performing essential functions for this group. The production control group is responsible for scheduling, monitoring, and running application software for the City's major production systems. Production control group employees also support the application system change control process by managing the transition of software between development, test, and production environments. We also determined that due to staffing shortages, the application programmers were moving their own work from the test environment to the production environment. In addition, we determined that 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.

B. We recommended that DFAS management 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.

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.

ACTION TAKEN

A. The audit recommendation has been fully implemented. DFAS hired two individuals for the production control group.

B. The audit recommendation has been fully implemented. On June 16, 2003, the CAO issued a memo requiring all departments advertising information systems positions to

use DFAS staff as subject matter experts for the development of technical interview questions and to participate as members of the interview panel.

OTHER ITEMS NOTED DURING THE FOLLOW-UP AUDIT

This additional item was noted during the follow-up audit.

Bio-park Life Support system replacement

We were told by Aquarium personnel that a new computer system called Continuum would be coming on-line for Tingley Beach in either the spring or summer of 2005, and that included a software application that would take the place of the Life Support system. The contract for this project is between The Department of the Army and the City of Albuquerque. We asked Bio-park management (management) if this new system had been submitted for review to the Technical Review Committee (TRC). Management told us that they did not submit this project to the TRC, and were not aware of this requirement.

According to the Albuquerque Code of Ordinance, 2-6-3-2 (D) et seq ROA 1994: Information Services Committee (ISC) – Duties, Responsibilities, and Powers, "Each city department shall prepare an information systems plan annually and submit it to the Committee for approval. In addition to reviewing these annual plans, the Committee shall also review, on an ongoing basis, all proposed information services activities for adherence to the Information Services Master Plan and to city-wide standards. No significant change in type or level of information services activities and no significant information services initiative shall occur without the approval of the Committee. The Committee shall establish a minimum level of information services activities which shall require review and approval by the Committee."

According to the contract between the Army and the City, the cost of the project will approximate $6.5 million. The contract does not provide detail on how the $6.5 million will be spent, and it is unclear what portion will be spent on information systems.

If Bio-park management does not submit information systems projects to TRC and ISC, proper procurement purchasing policies may not be followed.

RECOMMENDATION

CSD should ensure that all information services activities are reported to the Technical Review Committee and the Information Services Committee as required by Information Technology Policies and Standards, and the Albuquerque Code of Ordinances.

EXECUTIVE RESPONSE FROM CSD

"The Continuum software coming on-line at Tingley Beach is under the control of the Army Corp of Engineers, but can be monitored remotely from the aquarium. The Tingley system was engineered to match the existing, preapproved system at the aquarium."

AUDITOR'S COMMENT

Per the contract with the Army Corp of Engineers, the City was required to contribute 25 percent of the total project modification costs. The City's portion was projected to be $491,000. Since the information system was included in the cost of the project, CSD was required to submit a request to TRC.

xc: Accountability in Government Oversight Committee Members
Martin Chavez, Mayor
Gail Reese, Chief Financial Officer
City Councilors
Laura Mason, Director, Council Services Department
Jon Zaman, Policy Analyst II
Sandy Doyle, Director, Department of Finance & Administrative Services
Millie Santillanes, Director, Cultural Services Department
File