Office of the City Auditor

CONSENT CALENDAR
September 16, 2003

To: Honorable Mayor and Members of the City Council

From: Ann-Marie Hogan, City Auditor

Subject: Information Systems General Controls Audit

RECOMMENDATION

That Council request the City Manager to report back no later than February 17, 2004, regarding the implementation status of each of the Auditor's recommendations in the attached report, and to set a date for a follow up report to Council if any recommendations remain unimplemented at that time.

SUMMARY

A series of audits of the City's information technology was included in the Auditor's fiscal year 2003 audit plan, with the support of the City Manager and the Director of Information Technology. The attached Information Systems General Controls Audit was performed to evaluate the adequacy of physical controls, inventory controls, environmental controls, access security and recovery planning for the City's information systems. Audit fieldwork began on March 4, 2003, and concluded August 6, 2003. Some of the major concerns identified in the audit were:

- The City does not have a written security policy in place to provide guidelines on making specific decisions related to information systems security or to provide security procedures for users and system administrators to follow (Finding 1).
- Security controls to guard against unauthorized access to the City's information resources appear to be inadequate as evidenced by weak password protection (Finding 2), inadequate remote access controls (Finding 7), and terminated employees' user accounts not being removed or disabled (Finding 4).
- There is no disaster recovery plan for the network servers. In addition, backups for the network servers are not stored offsite (Finding 9).
- Activity logs or event logs are not reviewed regularly for possible security violations or system errors, reportedly due to limited staff resources. (Finding 6)
- Fire protection for the computer room at the Civic Center building is inadequate. The air conditioning in the room may not be functioning properly. (Finding 10)
- Critical computer equipment may be physically accessed by unauthorized City employees. (Finding 11.1 & Finding 11.2)
- The City has not yet completed a full and accurate inventory record of its computer equipment and software and there are no procedures in place to require departments to notify Information Technology of their computer equipment acquisitions. (Finding 12.1 and Finding 12.2)

2180 Milvia Street, Berkeley, CA 94704 ● Tel: (510) 981-6750 ● TDD: (510) 981-6903 ● Fax: (510) 981-6760
E-Mail: auditor@ci.berkeley.ca.us

FISCAL IMPACTS OF RECOMMENDATION

The audit did not look at the cost to implement the audit recommendations. We recommend immediate attention be given to establishing a Citywide security policy, to strengthening access controls, and to developing a disaster recovery plan for critical network servers.

CURRENT SITUATION AND ITS EFFECTS

The Department of Information Technology (IT) indicated that they have begun to take significant steps to improve security. Among them are drafting a comprehensive Network Security Plan, reviewing access rights for IT staff, deleting terminated user accounts, arranging off-site storage of backup tapes, and completing a desktop hardware inventory. Most recommendations are scheduled to be implemented no later than December 31, 2003, or earlier as specified in the report, except for the issuance of a written security policy that is scheduled to be drafted for management review by December 2003 and issued in final form by December 2004, the upgrade of the air conditioning in the computer room by May 2004 and the completion of the software inventory by November 2004.

RATIONALE FOR RECOMMENDATIONS

The fast growing information technology capabilities allow easy and convenient use of information systems to originate, process, store and communicate information. However, the ease and convenience come with new risks. Among these is the risk that valuable and confidential information may be lost, corrupted, misused or accessed by unauthorized persons. We must minimize this risk by developing a flexible security strategy that adapts to the changing environment to protect the City's information resources.

CONTACT PERSON

Ann-Marie Hogan, City Auditor
Office of the City Auditor, (510) 981-6750

Approved:

_____

Ann-Marie Hogan, City Auditor
Office of the City Auditor

City of Berkeley

Information Systems General Controls Audit

Prepared by:

Ann-Marie Hogan, City Auditor, CIA, CGAP
Teresa Berkeley-Simmons, Audit Manager, CIA, CGAP
Jocelyn Nip, Auditor II, CPA

Presented to Council September 16, 2003

2180 Milvia Street, Berkeley, CA 94704♦ Tel.: (510) 981-6750 ♦ Fax: (510) 981-6760

INFORMATION SYSTEMS GENERAL CONTROLS AUDIT
TABLE OF CONTENTS

		Page No.
I.	**EXECUTIVE SUMMARY**	1
II.	**OBJECTIVES OF THE REVIEW**	2
III.	**SCOPE AND METHODOLOGY**	2
IV.	**BACKGROUND**	2
V.	**FINDINGS AND RECOMMENDATIONS**	
Finding 1	There is no written security policy in place.	4
Finding 2	Current password composition does not offer strong password protection and network passwords never expire.	4
Finding 3	Network administrative rights are not restricted to network administrators.	5
Finding 4	Terminated employees' user accounts are not timely disabled or cancelled.	6
Finding 5	There are inconsistent practices in entering user "Full Name" when a new user account is created.	7
Finding 6	Activity or event logs are not reviewed regularly.	8
Finding 7	Security controls over access to the City's network through the Internet are not adequate.	9
Finding 8	Call-back is not set up for the modem line connection.	10
Finding 9	Backup tapes are not stored offsite and there is no disaster recovery plan for the network severs.	10
Finding 10	Fire protection for the computer room is inadequate and the air conditioning may not be functioning properly.	12
Finding 11.1	The computer room may be accessible by unauthorized employees.	13
Finding 11.2	System servers located outside the Civic Center building may not be secured.	14
Finding 12.1	There is not a complete and accurate inventory of the City's computer equipment and software.	14
Finding 12.2	Departments are not required to notify the Department of Information Technology (IT) of their computer equipment acquisitions.	15
VI.	**CONCLUSION**	15
REFERENCES		17
APPENDIX A:	Organization Structure of Information Technology	18
APPENDIX B:	Network Typology	19
ATTACHMENT:	Information Techology Accomplishments (Prepared by IT)	20

INFORMATION SYSTEMS GENERAL CONTROLS AUDIT

I. EXECUTIVE SUMMARY

We completed an Information Systems General Controls Audit which focused on physical controls, inventory controls, environmental controls, access security and recovery planning for the City's information systems. Three of the major concerns identified in this audit were:

1. The City currently does not have a written security policy in place to provide guidelines on making specific decisions related to information systems security or to provide security procedures for users and system administrators to follow (Finding 1). Due to the lack of written policies, some conditions identified in this report, although generally known, are not sufficiently addressed.

2. Security controls to guard against unauthorized access to the City's information resources appear to be inadequate as evidenced by weak password protection (Finding 2), inadequate remote access controls (Finding 7), and terminated employees' user accounts not being removed or disabled (Finding 4).

3. Although there is a disaster recovery plan for the AS/400, there is no disaster recovery plan for the network servers. In addition, backups for the network servers are not stored offsite (Finding 9). A timely recovery of critical information may not be possible in the event of an unexpected disaster.

We recommend immediate attention be given to establishing a Citywide security policy, to strengthening access controls and to developing a disaster recovery plan for critical network servers. Other findings identified in this audit were:

- Network administrative rights were not restricted to network administrators. (Finding 3)
- There are inconsistent practices in entering user names when a network account is created. (Finding 5)
- Activity logs or event logs are not reviewed regularly for possible security violations or system errors, reportedly due to limited staff resources. (Finding 6)
- No call-back is set up to authenticate dial-in location when a modem line is used to access the network. (Finding 8)
- Fire protection for the computer room at the Civic Center building is inadequate. The air conditioning in the room may not be functioning properly. (Finding 10)
- Critical computer equipment may be physically accessed by unauthorized City employees. (Finding 11.1 & Finding 11.2)
- The City has not yet completed a full and accurate inventory record of its computer equipment and software and there are no procedures in place to require departments to notify IT of their computer equipment acquisitions. (Finding 12.1 and Finding 12.2)

These concerns were discussed with Information Technology staff. We would like to express our appreciation for their input in identifying recommendations to resolve our concerns as well as for their cooperation and assistance provided to us during this audit.

II. OBJECTIVES OF THE AUDIT

The audit objective was to determine if general controls, especially security controls, in the information systems environment are adequate.

This audit was scheduled to be performed in the Auditor's fiscal year 2003 audit plan with the support of the City Manager and the Information Technology Director.

III. SCOPE AND METHODOLOGY

The audit focused on five areas: physical controls, inventory controls, environmental controls, access security and recovery planning. Methodology included review of existing City policies and procedures related to information technology, interviews with management and staff, and analysis of pertinent data and records. The period under review was fiscal year 2003. The last day of fieldwork was August 6, 2003, but testing was substantially completed prior to June 16, 2003. The audit was conducted in accordance with the Government Auditing Standards. Audit work was limited to those areas specified in the Scope and Methodology section of this report.

IV. BACKGROUND

The Department of Information Technology (IT) has a fiscal year 2003 adopted budget of $2,506,320. The current organizational structure of the IT department is presented in Appendix A.

Based on a report presented to Council by IT on April 1, 2003, the City has a Local Area Network (LAN) that connects 27 buildings. The center of the network consists of the Civic Center, the Permit Service Center, the Public Safety building, 1947 Center Street, and the Finance Service Center. These buildings are linked by under-ground fiber optic cable. The other buildings are linked to the network by leased T1 lines (fiber optic lines that carry data at high speed and plug into the network's routers).

According to the April report, the City utilizes 78 Dell servers and has approximately 1,027 personal computers throughout 20 departments. In addition, the City has approximately 200 notebook computers, plus other portable devices such as Palm Pilots and Pocket PCs. Microsoft Windows 2000 is the standard desktop operating system. Some older desktops continue to run on Windows 95, Windows 98 or Windows NT. The City's financial system, FUND$, runs on an IBM AS/400 mainframe. The Public Safety system runs on Hewlett Packard Alpha hardware and a smaller AS/400 computer. The City's network infrastructure is presented in Appendix B.

The IT department provides various degrees of technical and training support to the City's employees and departments. According to the April report, IT's principal functions include:

- Maintaining and developing the City's computer network.
- Providing support to desktop users.
- Maintaining the City's Web site and Intranet.
- Deploying and enhancing the City's phone system.
- Developing and maintaining the City's Geographic Information System (GIS).
- Maintaining and enhancing the City's financial system.
- Supporting and enhancing the Public Safety computer system.
- Specifying, acquiring, and developing departmental applications.
- Supporting the City's telecommunication policies.

Technical support is mainly provided via the Help Desk. The Help Desk currently utilizes an internally developed system to track and follow up on reported requests and problems.

The IT department entered into a one year contract with Convergent Computing in December 2000 to provide support services and trouble-shooting services for the City's computer network. Since then, the contract term has been amended three times. The contract amount has been increased from $40,000 to $120,000 and the current contract term expires on June 30, 2004.

As noted in the April report, *"virtually every member of staff who has a desk job now has a networked computer…"* Most City employees are granted access to the Internet, the City's Intranet, and the City's network. The City's policy on electronic mail (e-mail) is set forth in Administrative Regulation (A.R.) 4.2. Employees may also be granted access to FUND$ as required by their City duties. According to A.R. 2.6, supervisors are responsible for determining the appropriate level of access to the City's systems and requesting authorization for their staff through the IT department. IT will clear authorization for access to a specific module through the module leader and notify the supervisor and department director of approval. These service requests are processed on-line at the Help Desk section of the City's Intranet, iCoBWEB. If the request is for a new hire, the Help Desk will set up a new network user ID based on the request. If the new hire also needs to access FUND$, IT will forward the request to an AS/400 system administrator who will set up an AS/400 user account. Since there are multiple modules in FUND$, user capabilities are granted individually, based on needs as determined by the supervisor, either by an IT system administrator (IT staff responsible for directing the design, analysis, creation, monitoring, administration, troubleshooting, and enhancement of personal computer networks) or by a module leader (staff in the department which has responsibility for that module). According to A.R. 2.6, supervisors are also responsible for notifying IT when an employee is terminated or transferred so that system authorization may be timely cancelled or modified.

To access the City's financial systems (FUND$), a user has to log into the City's network using his or her assigned user ID. Access control to the network is therefore the first line of defense for the financial information which is processed on the AS/400 mainframe. This audit focused on network security. FUND$ security, on a module basis, will be addressed in more detail in a separate audit.

V. FINDINGS AND RECOMMENDATIONS

Finding 1: There is no written security policy in place.

The City currently does not have a written security policy in place. A written security policy is the basis for developing standards to safeguard computer equipment and data assets. It promotes uniformity and conformity across an organization. Without such a policy, the responsibility to control or to mitigate the risk of unauthorized access and misuse may be neglected.

Recommendation 1:

Develop a Citywide written security policy. One of the top ten recommended information security practices advocated by Internet Security Alliance includes: *"Create policies that address key security topic areas such as security risk management, critical asset identification, physical security, system and network management, authentication and authorization, access control, vulnerability management, incident management, awareness and training, and privacy."* [1]

City Manager's response:

IT agrees with the audit finding and the recommendation. Although there are policies and procedures in place for e-mail and FUND$ security, there is no comprehensive Citywide security policy. However, following recent changes to IT's organizational structure, the IT Department has commenced work on an enterprise computing security plan and will create a draft outline policy by December 31, 2003. A final written policy will be issued by December 2004. In the interim, there are a number of policies and procedures that can be quickly institutionalized and later incorporated into the final security policy. Specifically, FUND$ passwords will be required to conform to the stated strong password standard, the number of attempted logins will be reduced and physical security to the server room will be improved. Further, some policies have already been implemented, such as recommending that remote servers be housed in a secure, ventilated closet, and requiring IT approval for all hardware and software acquisitions.

Finding 2 Current password composition does not offer strong password protection and network passwords never expire.

According to A.R 4.2 that governs electronic mail, *"…Employees shall protect the City's security by regularly changing their private passwords."* However, this policy is not enforced because passwords are set to "never expire". Users are not required to change their passwords periodically. In addition, the network passwords are set to have a minimum of five characters. This is not in accordance with the "best practices" published by Microsoft which recommends strong passwords be of at least seven characters consisting of letters, numerals, and symbols.

There is also no composition requirement for the FUND$ passwords, although users are required to change their passwords every six months because they expire. In addition, ten unsuccessful login

attempts are allowed before the passwords are deactivated, exceeding the general practices of three to six attempts.

Strong passwords are important because computer hackers continue to improve their tools for cracking passwords. Weak passwords can be cracked in minutes by experienced hackers, increasing vulnerability to unauthorized access.

Recommendation 2:

2.1 Require all passwords to have at least seven characters consisting of letters, numerals, and symbols in accordance with Microsoft's "best practices" standards.
2.2 Require users to change their network passwords every three to six months.
2.3 Reduce the number of allowable unsuccessful login attempts to FUND$ to between three and six attempts.

City Manager's response:

IT agrees with the audit finding and recommendations.
2.1 IT will change the FUND$ password requirements by November 1, 2003. The network password change is more technically complex but will be completed by December 31, 2003.
2.2 Regular user passwords for FUND$ will be required to be changed every three months and more powerful passwords (QSECOFR, QPGMR, QHTE, etc.) will be required to be changed every month. Network passwords will be required to be changed every three months. Both changes will be made in the timeframe quoted in 2.1 above.
2.3 This will be changed to allow only four attempts and will be completed by October 1, 2003.

Finding 3 Network administrative rights are not restricted to network administrators.

Some Help Desk employees other than the network administrators have administrative rights to access restricted resources in the network, increasing the risk of unauthorized changes made to these resources whether by inadvertent human error or intentional tampering. During the course of fieldwork, the Network Administrator stated that this issue was addressed by immediately removing or disabling unneeded accounts from the "Domain Admins" and the "Administrators" groups.

Recommendation 3:

3.1 Review network access rights and functionalities for all IT staff. Remove unwarranted access or access that is not consistent with users' job responsibilities.
3.2 Perform periodic reviews of membership in the administrative groups to ensure no unauthorized group assignment is made.

City Manager's response:

IT agrees with the audit finding and recommendations.

3.1 IT removed unwarranted access or access that is not consistent with users' job responsibilities effective June 2003.

3.2 Review of membership in the administrative groups will be conducted quarterly beginning November 2003.

Finding 4: Terminated employees' user accounts are not timely disabled or cancelled.

Information used for the City's day-to-day operations is often captured, stored, and accessed in digital form. Digital data, therefore, must be made easily accessible, yet must also be protected from misuse. When new hires start to work for the City, they are assigned access to system resources based on their job responsibilities. However, when employees leave the City, their access is not always promptly cancelled. A.R. 2.6 "City Property – Issuance and Retrieval" requires that *"Supervisors must notify the Manager of Information Systems, (cc the Department Director) to cancel or modify access and/or authorization for the terminated or transferring employee by e-mail, or other means."* It appears that this procedure is not diligently followed. A user who is no longer employed by the City should not continue to have system access because it provides opportunities for unauthorized access. It also exposes the City to the risk of vengeful acts committed by disgruntled ex-employees.

A review of the User Manager (Microsoft administrative utility) revealed that there are over 2,600 network user accounts. By using Audit Command Language (ACL) audit software to match users' "Full Name" to the terminated employee names provided by Payroll Audit, the auditor identified 418 of these users whose employment had been terminated between January 1995 and April 2003 (The payroll software does not have records of employees terminated prior to 1995). The auditor further selected a sample of 38 from the 418 users and found that only 5% of the selected user accounts were disabled. Of the 38 sampled users, 79% continue to have access capability to the network and 16% of the accounts require password change at next login. In addition, after excluding the 418 user accounts identified above, over 400 of the remaining user names could not be tied to a current active City employee name. This may be because the employee was terminated prior to 1995, a different name was used or entered, or the name was mistyped.

We also reviewed the AS/400 users accounts. Out of 552 accounts, only 16 user names (less than 3%) are identified with a terminated employee name.

Recommendation 4:

4.1 Immediately remove all invalid user accounts and user accounts of terminated employees.

4.2 The responsibility for notifying IT of terminations and transfers should remain with the departments as required by A.R. 2.6. However, on a going forward basis, a designated IT employee should verify with Payroll Audit quarterly, as a cross-check, that terminated employees' user accounts are promptly disabled or removed. In addition, IT should advise the City Manager of departments failing to adequately notify the IT department of terminations and transfers.

4.3 The City Manager should issue a memo reminding the departments that it is their responsibility to timely notify IT of employee terminations and transfers.

City Manager's response:

IT agrees with the audit finding and recommendations.

4.1 In the past, user e-mail accounts were disabled by changing the password when a member of staff left the City, but the accounts themselves were left there in order to preserve e-mail and files for the Department Heads. IT now has alternative means to keep these materials without preserving the accounts. As a consequence, IT is now deleting terminated employees' accounts. IT will either disable or delete all terminated employee accounts by August 31, 2003.

4.2 Beginning November 2003 IT will review employee terminations and transfers and report to the City Manager, on a quarterly basis, the departments that fail to notify IT of the terminations and transfers.

4.3 A memo reminding the departments to timely notify IT of employee terminations and transfers will be issued by September 16, 2003.

Finding 5 There are inconsistent practices in entering user "Full Name" when a new user account is created, causing difficulties in identifying the account owner.

"Full Name" is a field on the Microsoft User Manager screen used to record a user's name when a new network account is created. Microsoft advocates that *"The full name is the user's complete name. It is a good idea to establish a standard for entering full names so that they always begin with either the first name (Louise G. Morgan) or the last name (Morgan, Louise G.)."* The Help Desk, however, does not have a consistent convention to enter an account owner's full name. Sometimes the last name is input followed by a comma and the first name. Sometimes the first name is input first followed by the last name. In some cases, Liz, Bill, and Ted are entered instead of Elizabeth, William, and Theodore, causing the full names to be different from the names appearing on the payroll records. These inconsistent practices make it very difficult to maintain or update user profiles based on employee names and status. The auditor was unable to identify all terminated employees by matching the "Full Name" to the payroll records because of these inconsistencies. The Network Administrator also indicated that he had difficulties in identifying account owners especially when there were duplicate names.

Recommendation 5:

Enter "Full Name" according to the names used for the Payroll records. We also recommend including the employee number in the "description" field to distinguish duplicate names.

City Manager's response:

IT agrees with the audit finding and the recommendation but plans to clear it with an alternative solution. The format of names should be the same, and IT will follow a standard for all new accounts. However, IT disagrees that "Liz" should always be "Elizabeth". Many members of staff

only use a shortened version of their name, and IT feels that peoples' desire as to how they wish to be addressed should be respected. However, IT agrees that clearly articulated protocols for account creation are necessary and will include such documentation in their security plan.

Finding 6 Activity or event logs are not reviewed regularly for possible security violations or system errors, reportedly due to limited staff resources.

Controls should be in place to ensure that a secure computer environment is maintained. One good control is the auditing function that is available in most operating systems. This function generates logs or reports that record activities or events such as access attempts, login failures and system performance that occur during the day or within a specified period of time. It is a tool that can be used to alert system administrators of system underperformance and possible security breach. A log can be configured to focus on particular users, objects or processes to serve a specific need. Currently, there is no procedure in place requiring these logs be reviewed regularly and it appears that existing activity data are not configured properly to facilitate meaningful review. Some logs are set up but are reviewed only when a problem occurs or is reported. The task of reviewing these logs can be personnel intensive. However, without the review, security violations and system underperformance may not be detected and rectified timely.

Microsoft advocates the use of audit logs as an effective security monitoring tool: "*Some good controls include violation and exception reports that help management determine, at a glance, whether their systems are being compromised. Many times, corporations run reports that log violations; however, running these reports in itself does not satisfy this control. Either the report is gathering too much information, the proper violations are not being filtered, or no one is reviewing the reports. These reports are another set of controls that help mitigate security risks throughout the corporation, but we often see them overlooked.*" [2]

Recommendation 6:

Configure event logs and exception logs and review them on a regular basis. According to Microsoft's best practices, *"… Auditing the system is not enough. In addition, the logs that hold the auditing information should be secured and maintained. In other words, security controls should be placed on the actual log files themselves to ensure confidentiality and availability when they are needed. …The best way to secure these files is to create an auditor group that has access to these files, and then take it away from all other groups. The people assigned to the auditor group will be responsible for maintaining the data within the logs."* [2] Therefore, access to these logs should be restricted to personnel that are assigned to maintain and review the logs.

City Manager's response:

IT agrees with the audit finding and the recommendation. However, reviewing all the logs is impractically time consuming. IT therefore will review sample logs about once a month and report on results quarterly. In addition, security that is being installed with the new AS/400 will provide a degree of automatic monitoring and allow audit reports to be run on demand by a variety of users.

Monthly documentation of review and quarterly reports on results will be available beginning November 2003.

Finding 7: Security controls over access to the City's network through the Internet are not adequate.

According to the Network Administrator, an employee who has to perform a City task from a location that is not connected to the network can request permission to access the network remotely by completing an authorization form. The form must be approved by his or her department director or the IT Director. All IT personnel are exempt from this requirement and are granted access automatically since their job duties often require them to access the network remotely.

There are 47 approved authorization forms filed with the IT department. However, over 150 users including IT personnel have accessed the network remotely according to a system report. Out of the 150 users, the auditor reviewed the employment status of 40 users. One user had been terminated in 1998 and three users had been terminated in 2002. The user profiles of these four employees indicated that they continue to have remote access capability to the network. Since "auditing" was not turned on at the time of the fieldwork, the auditor was not able to determine if these employees had accessed the network after they were terminated. "Auditing" was turned on by the Network Administrator in response to the auditor's request.

In addition, most City employees have remote access to their e-mail through the Internet. The remote e-mail server is located in the internal network. This setup opens a point of entry to the City's information resources from outside. The auditor found that any employee can log into the network through the Internet only if he or she knows the Uniform Resource Locator (URL) of the remote access server. The URL can easily be obtained from a co-worker who has the information. It appears that this information may have been shared by City employees since the number of users (150) greatly exceeded the number of authorization forms (47). This condition, coupled with weak password protection (Finding 2), terminated employees' user accounts not being cancelled promptly (Finding 4) and "auditing" not being turned on, cause the City's information resources to be very susceptible to unauthorized access.

Recommendation 7:

7.1 Add additional security controls or authentication requirements so that only authorized users can access the City's information resources remotely.
7.2 Review the remote access audit logs regularly to ensure only authorized employees have accessed the network from the Internet.
7.3 Issue a memo reminding City employees of the requirements or rules for network remote access.
7.4 IT should review the current network remote access policy in collaboration with Human Resources and incorporate changes in the new security policy.

City Manager's response:

IT agrees with the audit finding and recommendations.

7.1 The current WTS security protocols need improvement and IT plans to do so no later than December 2003.

7.2 IT will include this activity in the periodic review of the other logs and with review reports generated beginning November 2003.

7.3 The City Manager will issue a memo reminding City employees the requirements for network remote access by September 16, 2003.

7.4 *IT will review the current network remote access policy in collaboration with Human Resources; and incorporate the policy into the new security policy by December 31, 2003.*

Finding 8: Call-back is not set up for modem line connection.

Employees who work in locations that are not connected to the network can dial-in to the City's network through four phone lines. According to the Network Administrator, the current dial-in configuration enables an employee to dial-in to the network from anywhere and anytime. No call-back is set up to authenticate the dial-in locations. Call-back is a security tool used to verify that the incoming call is from a pre-defined phone line. The phone number can be configured as a part of the dial-in properties of the user account. Connection attempt is rejected if the call-back number of the incoming connection for that user does not match the configured call-back number. In the absence of strong password protection (Finding 2) and additional authentication requirements, the risks of unauthorized access through the dial-in phone lines are high.

Recommendation 8:

We recommend that IT set up call-back requirements for all dial-in connections through phone lines.

City Manager's response:

IT agrees with the audit finding and the recommendation. IT has been working toward eliminating modem connections throughout the City, and expects the few remaining modem connections to be replaced by leased T1 lines by November 2003, thus resolving the issue.

Finding 9: Network system backup tapes are not stored offsite and there is no disaster recovery plan for the network systems.

The simplest approach to recover critical data is to routinely make backup copies of the critical data. The backup copies are stored offsite in a different location so that the computer equipment and the data will not be destroyed all together when a disaster hits. A system disaster recovery plan is a documented and tested approach to restore IT operations and to recover critical computer processes and information from the backup copies in the event of a disaster.

AS/400 data

According to the Supervising Systems Analyst, there is a tested disaster recovery plan for the AS/400 mainframe, where most of the financial data resides. The plan was last tested two years ago.

The "System Recovery Procedure" documents the required procedures to restore critical files and applications. However, it does not include such important information as recovery site, vendor information, contact names and numbers, staff responsibilities during a disaster, and provisions for periodic testing and review. The backup procedures for the AS/400 are documented in the "AS/400 Backup Procedures". However, some information in the manual is obsolete and needs to be updated. According to the written procedures, the backup routines are run daily and monthly. The daily backup is run to copy specific production libraries and customized libraries that contain user data. The monthly backup is run on the first or second Saturday of each month to backup system related production libraries, system files and user profiles. Both the daily and monthly backup tapes are taken home for storage by an IT employee.

Network

There is no disaster recovery plan for the network systems and there are no written procedures for backing up network files. Backup routines are preset to run automatically daily and bi-weekly on a backup server located in the IT department. A few exchange servers located outside the Civic Center building have their own backup drives. An Information System Specialist has to go to these locations to change tapes or correct tape problems periodically. All backup jobs are centrally monitored by the network group in the IT Department. Backup tapes are stored in the same room where the backup server is located for about a week and then moved to the computer room for storage. In the absence of a disaster recovery plan and offsite storage of backups, it may be impossible to restore critical computer processes and information in the event of a major disaster.

Recommendation 9:

9.1 Store all backup tapes offsite. A more secured offsite storage, other than an employee's home, should be considered if it is economically feasible.

9.2 Develop written procedures for backing up network servers.

9.3 Develop a disaster recovery plan for critical network servers. The plan should provide for periodic testing of the backup processes.

9.4 Update the "AS/400 Backup Procedures". Refine the "System Recovery Procedure" to reflect such information as recovery site and available resources, names of personnel and their backup responsibilities, contact numbers, information on vendors who will provide support, and provisions to ensure periodic review, testing, and updating.

City Manager's response:

IT agrees with the audit finding and recommendations.

9.1 IT will investigate the feasibility of storing more tapes offsite.

9.2 IT will be installing new equipment in September 2003 to automate the entire network backup process.

9.3 A full-blown disaster recovery plan for the entire network, similar to what is already in place for the AS/400, would be very expensive. We must therefore first have a policy discussion with executive staff and Council to decide how far we want to go. The IT

Department will initiate this discussion later this year after it has further researched the options.

9.4 The "AS/400 Backup Procedures" will be updated by September 1, 2003, as recommended. Refining of the AS/400 "System Recovery Procedure" will be completed by October 1, 2003.

Finding 10: Fire protection for the computer room is inadequate and the air conditioning may not be functioning properly.

According to the Capital Improvement Programs Manager, the only fire protection devices in the Civic Center computer room are water sprinklers and smoke detectors. These are "general purpose" fire detection devices that are also installed in the rest of the building. Although water is an excellent fire suppressant, it also dampens sensitive computer equipment and is likely to cause irreversible damage. It does not appear to be the optimal solution for protecting computer equipment. In addition, the computer room generally has higher airflow meaning more smoke dilution than the rest of the building. A more sensitive detection device may be needed to provide early detection of a fire.

The air conditioning in the computer room may not be functioning properly to keep the room temperature at a desirable level. The optimal computer room temperature recommended by many experts is between 60°F and 70°F. One day the auditor observed that the outdoor temperature was around 65°F and the thermostat on the wall inside the computer room indicated 80°F. It was also noted that the temperature at the back of the room was even higher. Computer equipment is more prone to failure in high heat.

Recommendation 10:

10.1 Install a portable fire extinguisher in the computer room. The purpose is to increase the capability to extinguish a flame or fire immediately at early detection.

10.2 Complete a heat load analysis to determine if the existing air conditioning is functioning properly or is adequate.

10.3 Perform a risk analysis to determine an appropriate level of protection for the computer equipment. With budget limitations and other constraints, there may be conflicting priorities on expenditures. The cost of accepting a greater risk resulting from reduced expenditure must be carefully evaluated.

City Manager's response:

IT agrees with the audit finding and recommendations.

10.1 A portable fire extinguisher has been provided to IT and will be installed (permanently mounted) by Public Works by November 2003.

10.2 As the amount of equipment in the server room has grown, the air conditioning is not always adequate. IT has asked the Office of Capital Projects to upgrade the room's air conditioning by May 2004 when the weather will again start to place an unacceptable load on the server room's existing air conditioning system.

10.3 IT will perform a risk analysis by December 31, 2003.

Finding 11.1: The computer room may be accessible by unauthorized employees.

The computer room on the fourth floor of the Civic Center building is generally accessed with a pre-programmed swipe card. According to Public Works, a swipe card is programmed to access the computer room only when a written request approved by the Director of Information Technology is received.

The auditor obtained the names of the swipe cardholders, from Public Works, whose swipe cards have been programmed to allow access to the computer room. The auditor compared these names to the list of authorized employees provided by IT. Three cardholders were not on IT's authorized employee list. One of the three cardholders is a non-IT employee. It appears that some employees have been granted access to the computer room erroneously or that previously granted access rights have not been terminated based on access needs. According to A.R. 6.1, "*It shall be the responsibility of each department head to ensure that all building keys and access cards are retrieved from employees upon termination and/or if access to the building is no longer authorized.*"

Since the mainframe and most system servers reside in the computer room, access should be restricted to employees who need to perform their regular duties in the room. Inadequate access controls increases the risk of inadvertent changes to and intentional tampering with the systems.

Recommendation 11.1:

IT management should periodically review the cardholder log for the computer room, generated by Public Works, to ensure that only authorized employees have access to the computer room. If discrepancies are identified, IT should notify Public Works immediately to cancel unauthorized access rights.

City Manager's response:

IT agrees with the audit finding and the recommendation and will update the authorized employees list to include the two IT employees and remove access of the non-IT employee immediately. IT will also review the authorized user list with Public Works quarterly beginning no later than November 2003.

Finding 11.2 System servers located outside the Civic Center building may not be secured.

The auditor visited the Corporation Yard and observed that the servers were stored in an unlocked open area, increasing the risk for unauthorized access and theft. The same condition may exist in other locations.

Recommendation 11.2:

Require all servers to be locked in a cabinet at the minimum if a secured storage room is not available. Physical access should be monitored and limited to authorized personnel.

City Manager's response:

IT agrees with the audit finding and the recommendation. Whenever a server is installed at a remote site, the IT Department requests that a secure, ventilated closet be provided. Unfortunately, this doesn't always happen. Although IT currently attempts to monitor all server rooms during routine field visits, the department will institute a more directed monitoring schedule focused upon regular site assessments beginning December 2003. Public Works plans to install a vault to secure the existing servers located at the Corp Yard by December 2003.

Finding 12.1 There is not a complete and accurate inventory of the City's computer equipment and software.

The auditor requested an inventory list of the City's computer equipment and software from IT. According to the Senior System Analyst, IT is working with each department to prepare a complete inventory of all desktops and printers. According to IT, the inventory list was approximately 50 to 60 percent complete as of May 2003. If the City does not keep track of the computer equipment it owns, it is very difficult to effectively safeguard its assets.

Recommendation 12.1:

Complete an inventory of the City's computer equipment, including desktops, printers, laptops, firewalls, routers, servers and software etc. The inventory report should contain an unique identification number or serial number for each item and the report should be updated once a year. In addition, if unused or obsolete computer equipment is identified during the inventory process, IT should make appropriate arrangement to dispose the equipment as prescribed by A.R. 3.5 – Disposal of Surplus Property.

City Manager's response:

IT agrees with the audit finding and the recommendation. The inventory of desktop hardware has been updated and is currently being reviewed for accuracy by individual departments. For the first time, the City now has an online computer inventory available to Department Directors for regular monitoring of desktop inventory. Updates are made on a regular basis with yearly Department Directors reviews beginning July 2003. A mechanism for automation of software inventory has been deployed to 70% of the network by IT and will be completed by November 2004.

Finding 12.2: Departments are not required to notify IT of their computer equipment acquisitions.

Departments may purchase desktops, printers or other computer equipment without notifying the IT department. The latest published guideline on computer purchase can be found in the "Berkeley Matters" issued on June 3, 2003, by the City Manager:

IV. COMPUTER PURCHASE GUIDELINES

The purchasing of new computers and printers for use in the City should, under normal circumstances, be confined to the equipment options that are detailed on iCoBWEB. When circumstances suggest that non-standard technology is necessary, the individual responsible for making such a purchase is advised to first call Help Desk for direction. The Department of Information Technology may not support equipment ordered without adherence to this policy!"

This guideline gives departments the options of acquiring computer equipment without first consulting the IT department. This practice may result in departments acquiring equipment that is not compatible with the City's systems, making it very difficult for IT to track and support computer equipment for the City.

Recommendation 12.2 for the City Manager and departments :

Require departments to obtain sign-off from IT on all acquisitions of computer equipment used for City businesses.

City Manager's response:

IT agrees with the audit finding and the recommendation. The Purchasing Division of Finance has recently implemented a protocol designed to insure that IT is informed of all requisitions for hardware and software before a Purchase Order is issued. Staff will determine the most effective way to ensure that IT signs off on all computer equipment and software purchases by November 2003.

VI. CONCLUSION

The results of this audit indicated that the City needs to strengthen its system security to ensure a secure computer environment is maintained and its information resources are properly safeguarded.

"Security is an important part of a system infrastructure. An information system with a weak security foundation will eventually experience a security breach. Examples of security breaches include data loss, data disclosure, loss of system availability, corruption of data, and so forth. Depending on the information system and the severity of the breach, the results could vary from embarrassment, to loss of revenue, to loss of life." [3] With increasing dependence on information technology to carry out day-to-day operations, a flexible security strategy that adapts to the changing environment is required to protect the City's information systems and data. Information security is a continuous process to develop and implement security solutions. Although it is impossible to achieve 100% security, an adequate level of system security can be achieved through prioritizing and by standardizing policies. The success of such policies heavily depends on management's commitment and technological support for enforcing the policies.

REFERENCES:

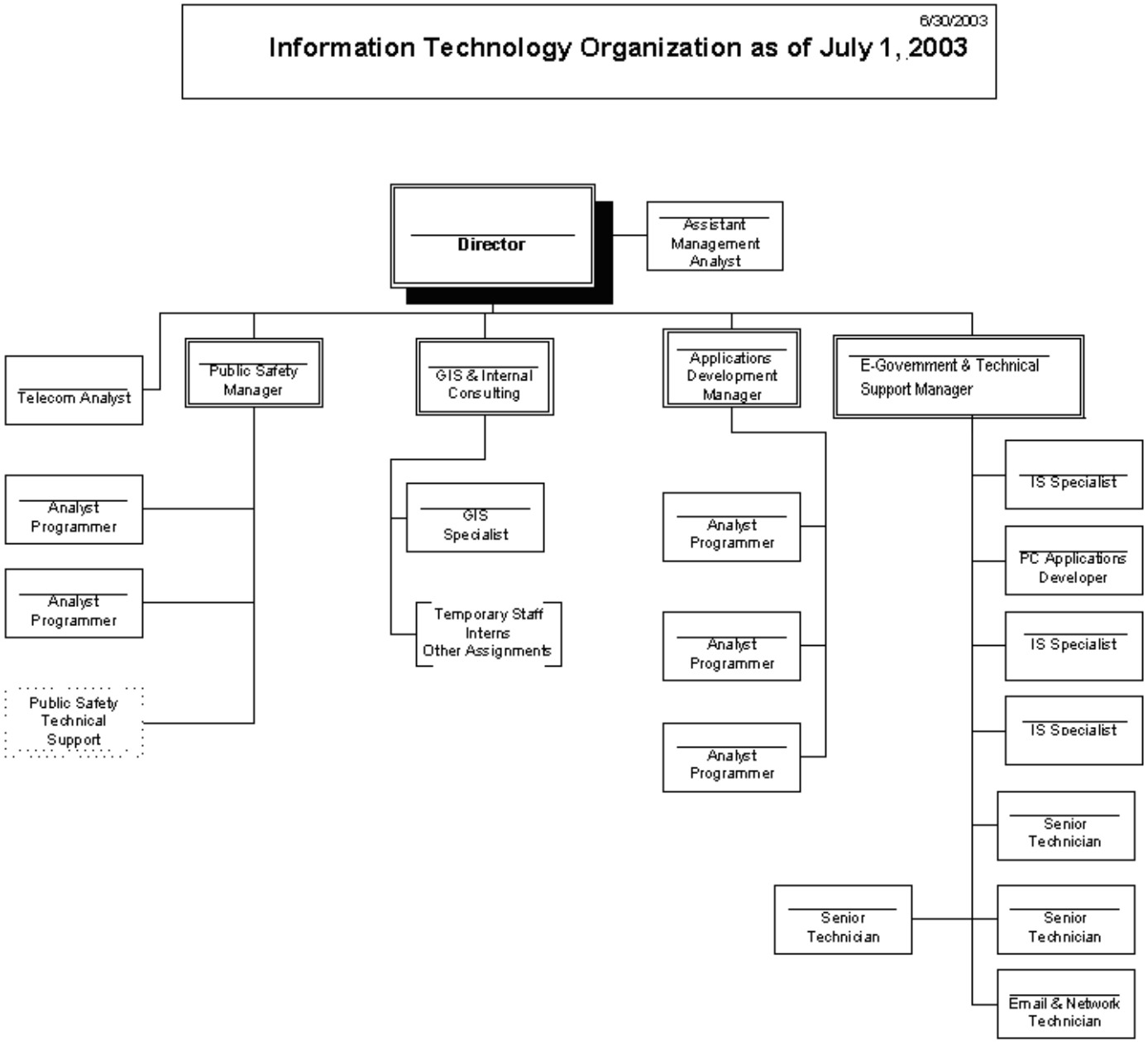
[1] Internet Security Alliance. Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices, 1st Edition - July 2002, P. 7.

(The Internet Security Alliance was created in April 2001 to provide a forum for information sharing and thought leadership on information security issues. Its mission is to use the collective experience of the members of the Internet Security Alliance to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems.)

[2] Microsoft Technet. Effective Security Monitoring (Chapter 4 from Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press), P. 1 & P. 26. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/network/ch04.asp

[3] Microsoft Technet. Window 2000 Operations Guide Series: Network Administration Operating Guide. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/opsguide/opsguide.asp

Source: Department of Information Technology **APPENDIX A**



City of Berkeley Network as of April 1, 2003 **APPENDIX B**

Source: Department of Information Technology

(This page is left blank)

Department of Information Technology

August 18, 2003

To: Ann-Marie Hogan, City Auditor
From: Chris Mead, IT Director

SUBJECT: INFORMATION SYSTEMS GENERAL CONTROLS AUDIT

The purpose of this memorandum is to record some general comments regarding your audit – our detailed responses are included in the main body of the audit following each finding.

First please let me state that I am grateful to you and your staff for performing the audit, as it has highlighted many deficiencies in our current security. I speak on behalf of my entire Department when I say that we feel chastened by your findings, and we are totally committed to rectifying our shortcomings. To this end, I have made a secure and resilient system one of the key strategic goals in our new Information Technology Master Plan.

In our responses to your findings, you will see that we have already begun to take many steps to improve our security. The most important of these steps is the recent reorganization of the I.T. Department that places our network group under stronger management by combining it with our User Support and E-Government Division. The manager of the new team, Donna LaSala, has made an excellent start by immediately drafting a comprehensive Network Security Plan that we have already begun implementing and should be completely executed by December 2003.

Among the other corrections we have already made are: the review of access rights for I.T. staff; immediately deleting terminated user accounts; arranging off-site storage of tapes; we have completed the inventory of PCs, which is now available online; and we are reviewing all hardware and software purchase orders.

Finally, I would like to say that I appreciate the thoroughness and professionalism that your staff has brought to this audit, and we look forward to working with the Auditor's Office to enhance the security of the City of Berkeley's systems.

Cc: Weldon Rucker, City Manager
I.T. Division Managers
Teresa Berkeley-Simmons, Audit Manager, Jocelyn Nip, Auditor II