OFFICE OF THE CITY AUDITOR
REPORTING ON ACCOUNTABILITY WITH A CITIZEN FOCUS

LOGICAL SECURITY OF THE CITY'S LOCAL AREA NETWORK

AUDIT REPORT #0201

October 2001

CITY OF TALLAHASSEE

Copies of this audit report #0201 (project #0101) may be obtained from the City Auditor's web site (http://talgov.com/citytlh/auditing/index.html), by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (dooleym@talgov.com).
Audit conducted by:
Beth Breier, CPA, CISA, Senior IT Auditor
Sam M. McCall, CPA,,CIA, CGFM, City Auditor

CITY OF TALLAHASSEE

CITY HALL
300 S. ADAMS ST.
TALLAHASSEE, FL
32301-1731
850/891-0010
TDD 1-800/955-8771

SCOTT MADDOX
Mayor
STEVE MEISBURG
Mayor Pro Tem

JOHN PAUL BAILEY
Commissioner
CHARLES E. BILLINGS
Commissioner
DEBBIE LIGHTSEY
Commissioner

ANITA R. FAVORS
City Manager
GARY HERNDON
Interim City Treasurer-Clerk

JAMES R. ENGLISH
City Attorney
SAM M. McCALL
City Auditor

MEMORANDUM

To: Mayor and Members of the City Commission

From: Sam M. McCall, City Auditor

Date: October 26, 2001

Subject: Audit Report on Logical Security of the City's Local Area Network (#0201)

We have completed an audit of the Logical Security of the City's Local Area Network (#0201). We submit this report that contains our audit issues and recommended actions and the responses from the City Manager and the Interim City Treasurer-Clerk. We will periodically review the implementation of these recommended actions.

We worked with many departments across the City within the offices of the City Manager and City Treasurer-Clerk. We thank everyone for their cooperation and assistance during this audit. If you have any questions or need a more detailed briefing on this audit, please contact me.

Respectfully submitted,

Sam m. mc Call

Sam M. McCall
City Auditor

SMM/mbd
attachment

Copy: Members of the Audit Committee
Appointed Officials
Executive Team
Donald C. DeLoach, Chief Information Systems Officer
Terald Baker, Technology Infrastructure Administrator
Walter McNeil, Police Chief
Thomas Quillin, Fire Chief
Gary Brinkworth, Manager – Utility Services
Pete Koikos, Director – Energy Services
Robert Herman, Director – Growth Management
Gloria Hall-McNeil, Director – Human Resources
Paula G. Cook, Records Administrator

Table of Contents

Audit Report

CITY OF TALLAHASSEE

Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Logical Security of the City's Local Area Network"

Report #0201 *October 26, 2001*

Executive Summary

There are two basic types of security controls that together can protect information resources: physical and logical. Physical security controls address restricting access to the location where computer hardware and equipment are housed. Logical security controls address restricting access into specific information systems and applications so that only authorized individuals can perform functions on the system.

This is the second report addressing the security of the City's information resources (also referred to as the City's local area network or LAN). The first report addressed the physical security controls of the City's LAN (Report #0106 issued in December 2000). The purpose of this second report is to address the logical security controls protecting the City's LAN.

The scope of this audit is limited in that our audit procedures: 1) included basic, but not extensive, vulnerability assessment activities (to identify potential access weaknesses) and no penetration testing (to obtain unauthorized access); and 2) did not include detailed database security testing.

During the period December 2000 through June 2001, the City Auditor's Office conducted an evaluation of the logical security controls that protect the City's LAN resources. The purpose of this report is to present the issues identified and the associated recommendations. In addition, we have provided Information Systems Services (ISS) management and the appropriate departmental staff with detailed information related to the logical security weaknesses identified during the audit. Evaluations of security programs for information technology resources are exempt from public record to prevent improper disclosure of information that could result in unauthorized access, modification, and/or destruction of information resources, such as equipment, programs, and data.[1]

The issues identified in this audit are provided below.

Written policies and procedures addressing information security are needed

Policies and procedures that address information security have not been implemented. ISS management has drafted written policies and procedures to address the logical and physical security of the City's computer resources, but these have not yet been completed, approved, and implemented. We recommend that ISS complete and implement these important information security policies and procedures.

An information security manager is needed

A person(s) has not been designated to manage the information security activities throughout the City. Without someone designated to perform information security activities, the risk is increased that the City's information technology resources could be damaged or destroyed by unauthorized persons, internally or externally.

User access and password controls need to be improved

Based on the results of our user access testing, we:

- concurred with ISS management that there were some areas that need improvement. These included user access administration for the network and remote access;
- noted that the password controls ISS management believed to be in place were not working as intended;
- noted that network user IDs were not being removed in a

[1] Section 119.07(1)(o), *Florida Statutes*

timely manner, and that the network user IDs were being shared among current employees;

- noted that remote access controls need to be improved; and
- noted that users were assigned privileged access capabilities that did not appear to be necessary for their positions.

Confidential data needs to be better protected from improper disclosure

We noted that confidential data, as defined by Chapter 119.07, Florida Statutes (F.S.) was not being adequately protected in the City's various information systems to prevent improper disclosure.

Appendix B provides management's action plan to address these identified issues. We would like to thank staff from ISS and all the departments that own and utilize application systems that provided support and assistance during this audit.

ISS and other departmental representatives have been very responsive and have corrected many of the identified access weaknesses

ISS and other departmental representatives have been very responsive to correcting user access weaknesses identified during the audit. We recommend that management continue to implement policies, procedures, standards, and processes toward the prevention, detection, and correction of information security weaknesses.

Audit Report

CITY OF TALLAHASSEE

Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Logical Security of the City's Local Area Network"

Report #0201 *October 26, 2001*

Purpose

There are two basic types of security controls that together can protect information resources: physical and logical. Physical security controls address restricting access to the location where computer hardware and equipment are housed. Logical security controls address restricting access into specific information systems and applications so that only authorized individuals can perform functions on the system.

This is the second report addressing the security of the City's information resources (also referred to as the City's local area network). The first report addressed the physical security controls of the City's Local Area Network (LAN) (Report #0106 issued in December 2000). The purpose of this second report is to address the logical security controls protecting the City's LAN.

Scope and Objectives

The scope of this audit includes the logical security of all identified access paths into the City's LAN. Fieldwork took place from December 2000 through June 2001.

Our objectives were to:

- obtain a general understanding of the network operations and the logical access paths into the network;
- provide assurances regarding security controls management believed were in place;
- evaluate the adequacy of security controls that

management believed should be improved;

- determine the adequacy of policies and procedures related to unauthorized access into the City's LAN;
- determine the adequacy of the controls in place to prevent unauthorized access in the City's LAN; and
- determine the accessibility to confidential information stored on the City's LAN.

The scope of this audit is limited in that our audit procedures: 1) included basic, but not extensive, vulnerability assessment activities (to identify potential access weaknesses) and no penetration testing (to obtain unauthorized access); and 2) did not include detailed database security testing. Our methodology is provided in Appendix A.

Background

City's Computing Environment

The City relies on computers and electronic data to perform functions that are necessary to provide services to the citizens of Tallahassee. Examples of these services include police and fire dispatching and reporting; electric, water, gas and solid waste operations; public works operations (traffic, streets and drainage); growth management and permitting; bus operations; and financial reporting.

City is Migrating from a Centralized to a Decentralized Computing Environment

The City, like other government and private industries, is migrating from a centralized mainframe environment to a decentralized (or distributed) client/server environment. In a mainframe environment, all users are connected to one central location for the hardware, software, and data; and management, authority, budget, and responsibility are centralized in one location, typically within the Information Systems Services division.

In the client/server environment, all users (also called clients) are connected to one or more servers. This client/server environment is replacing the mainframe environment that has been prevalent during the past 30-40 years. The design of the client/server environment distributes the functionality of the mainframe, including programs and data, primarily to the server and secondarily to the users' computers. This environment is based upon concurrent processing that increases the flexibility and power at the users' desktops.

The distributed client/server environment operates on a local area network (LAN). A LAN is a communication network that serves many users within a geographical area and consists of servers, workstations, a network operating system, and communications links. As communication technology advances, the number of ways in which users can connect to the servers increases. These paths include:

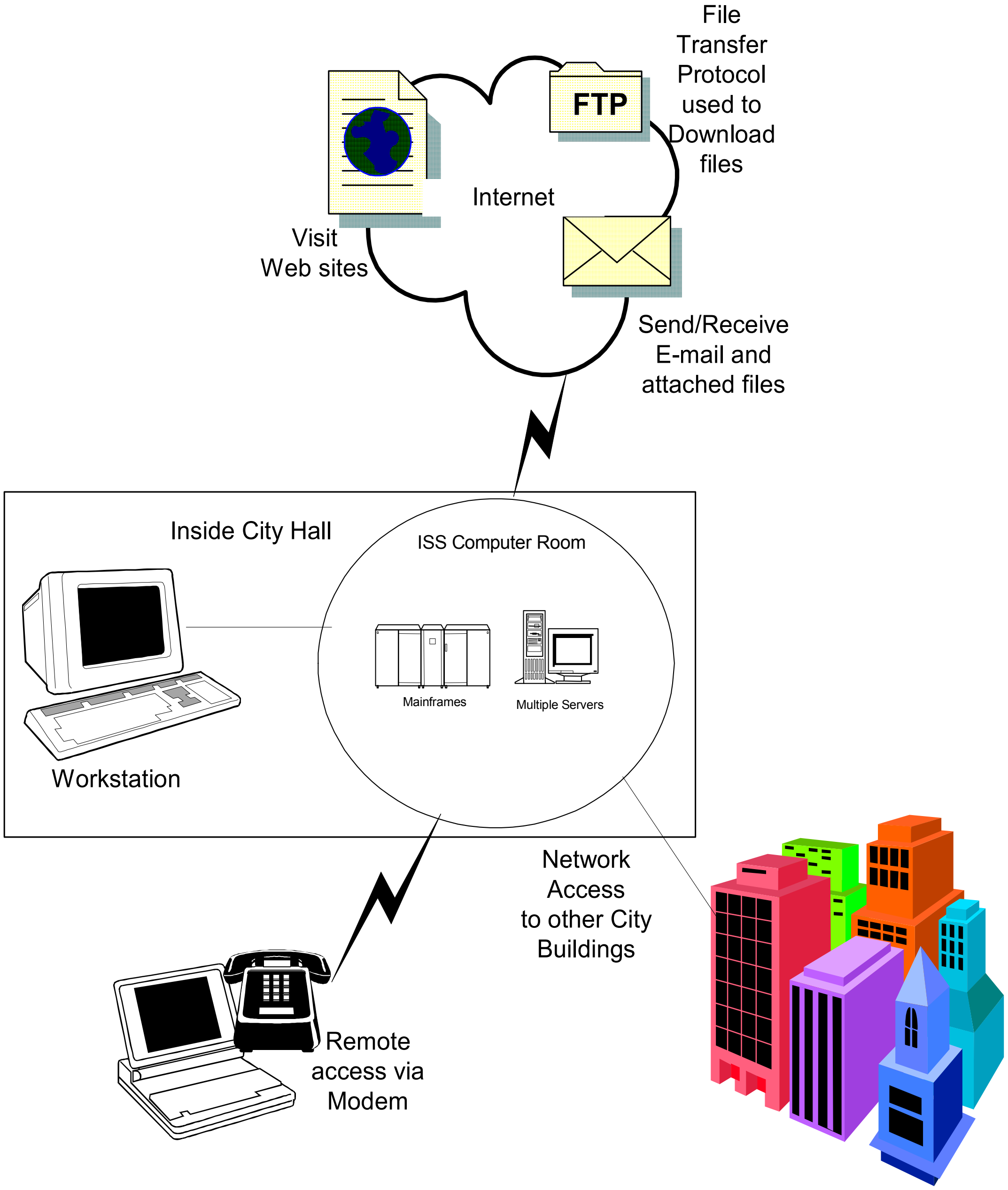
Access Paths into the City's Local Area Network

- direct login from employee workstations at the main building
- remote login from employee workstations at other City buildings via fiber or other transmission connectivity
- remote login via modems
- e-mail
- Internet

Though greater use of interconnected systems provides significant benefits through improved government operations, such systems are much more vulnerable to unauthorized intruders. Those intruders may manipulate data to commit fraud, obtain sensitive or confidential information, or severely disrupt operations.

Figure 1, on the next page, shows the different access paths into the City's LAN.

Figure 1
Access Paths into the City



Source: Developed by Audit Staff

Defining Logical Security

Security of information systems can be defined as the control structure established to manage the integrity, confidentiality, and availability of information systems data and resources.[2] There are two basic types of security controls that together can protect data and resources:

> ***Physical security -*** restricting access to the location where computer hardware and equipment are housed, as well as protecting the hardware and equipment against environmental hazards.
>
> ***Logical security*** **-** restricting access into specific information systems and applications to prevent unauthorized individuals from accessing programs and data.

A security breach occurs when information security policies are violated and someone has obtained unauthorized access into the network. Breaches can be suspected or actual and can relate to physical or logical security.

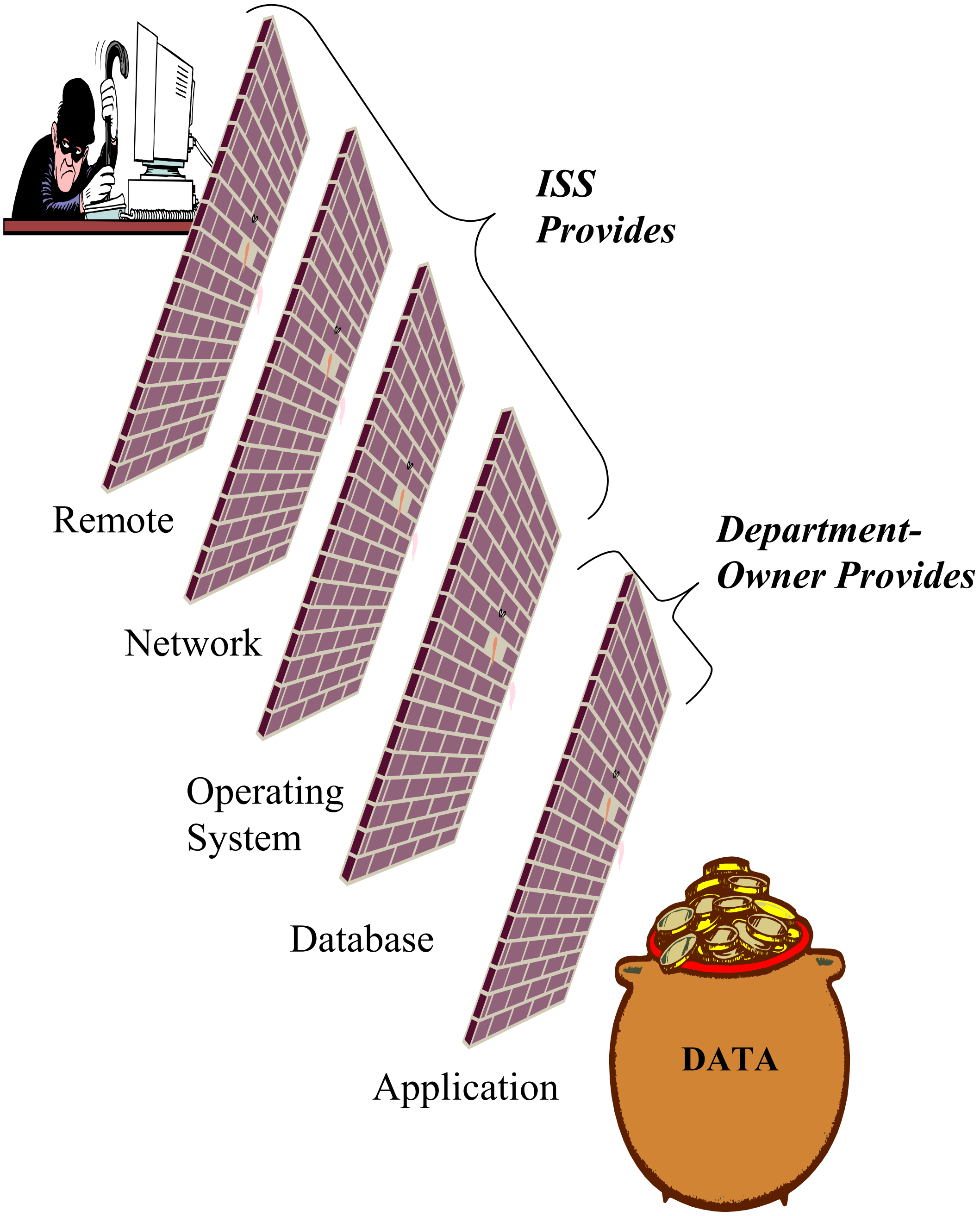
Responsibility for Logical Security exists at different technology layers and within different divisions

The responsibility for logical access controls into the City's information resources exists at different technology layers and within different City departments. Figure 2, on the next page, shows the various layers of logical access controls needed to adequately protect programs and data.

While each logical access layer is important, protection of the three outer layers, **remote**, **network**, and **operating system,** is crucial because these layers provide barriers to external attempts into the City's LAN. The ISS Distributed Network Section (DNS) is responsible for the security and maintenance of these three layers. ***Remote***

[2] Systems Auditability and Control, Module 9 "Security," Institute of Internal Auditors Research Foundation

Figure 2
Logical Access Layers that Protect the City's Data



Source: Developed by Audit Staff

access involves accessing the network from another PC from another city building or other location by modem, fiber, or other connectivity; and for accessing the network via the Internet or e-mail use.

The primary objective of ***network*** security is to provide a secure communication path to transmit information between interconnected host computer systems.[3] Host computer systems consist of primary computers in a distributed or multiple computer system. Database access and access to the network are controlled by the host computer. Network security includes designing, implementing, and monitoring access controls of network hardware (i.e., routers, switches, hubs, bridges).

In addition, DNS is responsible for access security related to data and programs at the ***operating*** system level (i.e., WindowsNT, mainframe, UNIX). Typically, additional software that solely provides user access security is used at this layer to strengthen operating system security.

The ***database*** layer of access security is the responsibility of the Database Administrators (DBA) within the ISS Applications Systems Section. The programs and data that unauthorized intruders may be attempting to access is located in databases. Access to the programs and data through the database application rather than the user's application (i.e., Financials, Human Resources, Customer Information System) can also be referred to as accessing the data behind the application or via the "back door."

ISS is considered the custodian of the data and is responsible for securing access to the data via the database

[3] Handbook of IT Auditing, 2000 Edition

software. It requires a high level of information technology expertise to manage security at the remote, network, operating, and database layers.

Access controls within software ***applications*** (i.e., payroll, financials, human resources, utility billing, risk management) provide yet another level of security for users of the application. While ISS is the custodian, the owner of the programs and data is whichever department(s) is identified as the primary business user. For example, the department-owner of the Financials system would be the Department of Management and Administration, since their primary business responsibilities include accounting, budgeting, and procurement.

The department-owner is responsible for specifying the level of application security required for their operations and supporting information systems, determining who is given access to their application system and what transactions they can perform, such as inquiry only, add, change, and/or delete. The department-owners are also responsible for protecting their own application passwords and related equipment. When users access the data through an application, it can be referred to as accessing the data via the "front door."

Managing the security at the application level does not require the level of technical expertise needed to manage the remote, network, operating, and database layers.

Unauthorized external users (also referred to as "hackers") trying to access an organization's information systems will most likely attempt to gain access via the remote, network, and operating system layers. Hackers will attempt to gain privileged access (as a system administrator) of the operating systems. Internally, most access weaknesses arise from users being assigned inappropriate access capabilities to any of the layers: remote, network, operating system, database, and/or application.

Logical access controls are to ensure that access to systems, data, and application programs is restricted to authorized users

The goal of logical access controls is to ensure that access to systems, data, and application programs is restricted to authorized users and takes into consideration:[4]

- authorization – are there measures in place to ensure that only authorized users are accessing the system?
- authentication – are there controls in place to ensure that the transmission received is sent by whom it says it is?
- user profiles and identification – are there controls in place to manage user access profiles and security assignments? Can the user accessing the system be accurately identified? Does the user access profile allow the user to perform only the functions assigned? Are the assigned access privileges appropriate?
- incident reporting and follow-up – are there controls in place to monitor, track, analyze, and report suspected and actual security breaches (i.e., unauthorized access into computer equipment locations or information systems)?
- cryptographic keys – are there controls in place to manage encryption keys used for internal and external transmission activity?

Logical access requires a balance of organizational policies, security administration guidelines, technical standards, and user procedures

These logical access components are implemented by managing a balance between policy at the organizational level, guidelines for security administration, and standards that address the technical configuration of the system components, and procedures for end users.[5]

[4] Control Objectives for Information and Related Technologies Audit Guidelines, 1996

[5] Handbook for IT Auditing, 2000 Edition

Issues and Recommendations

The purpose of this report is to present the issues identified during the audit along with associated recommendations. In addition, we have provided ISS management and the appropriate departmental staff with details of the security weaknesses identified during the audit. Evaluations of security programs for information technology resources are exempt from public record laws to prevent improper disclosure of information that could result in unauthorized access, modification, and/or destruction of information resources, such as equipment, programs, and data.[6]

Below is a description of the general issues identified and categorized in the following areas: security management and monitoring, user access controls, and protection of confidential data.

Security Management And Monitoring

Policies and Procedures Addressing Logical Security of the City's Network Should be Developed and Implemented

Policies and procedures have not been developed to address the logical access security to the City's information technology resources

Currently, written policies and procedures have not been implemented to address the logical access security to the City's information technology resources. ISS management has drafted written policies and procedures to address the logical and physical security of the City's computer resources, but these have not yet been completed, approved, and implemented.

An effective security program must begin with the implementation of policies, standards, procedures, and guidelines. Security policies fall into two categories: technical and administrative.

[6] Section 119.07(1)(o), *Florida Statutes*

Technical policies address the network architecture, hardware, and software. These policies typically affect how information technologies are protected and should include minimum standards for preventing information security breaches as well as procedures for detecting and correcting any vulnerability. Technical policies are most likely used by ISS and by those individuals responsible for designing and maintaining the network architecture.

Administrative policies address the processes that are to be carried out by people using and managing the information systems and should be communicated to all persons that use the City's information systems. Examples of the areas that should be addressed in an information security policy for logical access include the administration and security of:

Examples of logical security controls that should be included in an information security policy

User Rights and Responsibilities – determining who should be assigned access to the network and their access rights

Administrator Rights and Responsibilities – defining who is assigned this privileged access and what are their responsibilities

Passwords – defining the minimum password controls, such as the minimum and maximum length, composition, expiration period, use of previous passwords, initial login rules

Operating system – what security rules are set in the operating system, who has the access to change security rules and how changes are managed

Network architecture – what are the business rules for the network-related hardware and software. For example, firewalls/routers rules should dictate what types of transactions are allowed into and out of the network

Security monitoring – monitoring security activities for each vulnerability area identified by management; determining what information is logged, how, and where the logs are stored and who has access to them

Security awareness – conducting activities to promote user understanding regarding the importance of information security, and user activities to ensure that information is adequately secure

Viruses – to prevent the spread of computer viruses, detect and eradicate a virus that has infiltrated a PC or the network in a timely manner

Dial-up (Remote) connections – approval, acquisition, inventory, and access security rules related to the use of modems to access the network; process to request and implement other remote access paths to the network via fiber or other connectivity

Internet/E-mail Usage – obtaining access capabilities to access Internet, appropriate business use, downloading procedures

Application and Data Security – identifying owners of the data, defining the security requirements for the application programs and data, assessing the confidentiality of data, determining and implementing the security requirements for that data

Backups – process for identifying what systems are backed up, how often, and how often are they verified; and where they are stored and secured

Internal Control Guidelines (Administrative Policies and Procedures #630) states that internal control may consist of procedures, policies, information guides, and department operation guides. "Policies establish the organization's direction, while procedures indicate how policies are to be implemented and followed..…Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment."[7]

Policies are written at a broad level, therefore organizations also need to develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify the technologies and methodologies to be used to secure systems, while

[7] Systems Auditability and Control, Module 2 "Audit and Control Environment," Institute of Internal Auditors Research Foundation

procedures are more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures are then disseminated throughout an organization via handbooks, regulations, training and/or manuals.[8]

Without effective policies and procedures, there are no guidelines for City departments to follow to ensure that computer resources are protected against malicious or inadvertent acts resulting in a disruption of critical operations and services.

ISS is currently developing information security policies and procedures but they have not yet been adopted and/or implemented

As stated above, ISS management has drafted written policies and procedures to address the logical and physical security of the City's computer resources, but these have not yet been completed, approved, and implemented. We recommend that ISS complete and implement these important information security policies and procedures.

An Information Security Manager(s) Should be Formally Designated to Manage Information Security Activities in the City.

Currently, ISS conducts some network security activities, and some executive owners provide some application security, but there is no person or section designated to manage the information security activities throughout the City. Important logical security activities currently not being performed include:

Examples of Information Security Activities that are not currently being performed

- ♦ coordinating and conducting information security awareness training for employees;
- ♦ routinely monitoring security activities, such as suspected or actual security breaches;
- ♦ recording, tracking, and analyzing suspected and actual information security incidents; and

[8] U.S. Dept. of Commerce National Institute of Standards and Technology "An Introduction into Computer Security: The NIST Handbook," 800-12.

- assisting department-owners in assessing the confidentiality and security requirements of their data (also called assessing risks).

In addition, an information security manager(s) could assist departments in identifying and assessing physical security weaknesses at locations housing LAN equipment throughout the City.

Security-related responsibilities of offices and individuals throughout an entity that should be clearly defined include (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administration.[9]

Without a person(s) designated to be responsible for the information security activities, there is no assurance that information security is being considered, evaluated, or monitored in the City. This increases the risk that the City's information technology resources could be damaged or destroyed by unauthorized persons, internally or externally.

During the fiscal year 2002 budget process, ISS management requested funding for additional positions, to include an Information Security Manager. Funding was approved for four positions; however, the Information Security Manager position was not identified by ISS as one of the four positions to be filled in the 2002 budget year.

Recommendation Related to Managing Information Security

We continue to recommend that management formally assign the responsibility for assuring security of the City's information resources to an information security manager(s), reporting to senior management. This person(s) should be independent of the departments that manage and maintain

[9] Federal Systems Controls Audit Manual, Volume 1, "Financial Statement Audits," U.S. General Accounting Office

the systems and facilities that require information security.[10] Such responsibilities would include: overseeing the implementation of information security policies and procedures, assessing security risks and recommending corrective actions, increasing security awareness by City employees, monitoring security measures, and reporting to senior management.

User Access Controls

User access controls are security controls that limit a person's access to data and programs and can include the:

- user IDs, such as defining a standard format, assigning and removing user IDs;
- passwords, such as defining a standard composition (alphanumeric combinations), the minimum and/or maximum length, lifespan (i.e., 45 days before the user is required to change); and
- the administration of individual user access capabilities, such as assigning specific locations the user can and cannot access, or what transactions the user can perform (i.e., inquiry, add, delete, change)

To evaluate the adequacy of those access controls, we conducted various tests to determine where basic user access and password controls were in place and working effectively.

Based on the results of our testing, we:

- concurred with ISS management that there were some areas that needed some improvements. These included user access administration for the network and remote access;
- noted that the password controls ISS management believed to be in place were not working as intended; and

[10] Control Objectives for Information and Related Technology, Information Systems Audit and Control Foundation, 1996

- noted there were a number of users with privileged access capabilities that do not appear to be necessary for their position.

The results of our testing are provided below according to the type of user access areas: network user IDs, remote user access, passwords, and privileged access capabilities.

Network User IDs should be removed in a timely manner for terminated employees and should not be shared among current employees.

Weaknesses identified related to the management of Network User IDs

1. There has not been an effective process in place to remove user IDs from the network in a timely manner. During the period of January 1999 through January 2001, there were 524 terminated employees. Of the 102 terminated employees we tested (19%), we identified 30 active network user IDs (29% of those tested). Of those 30 terminated employees with active network user IDs, we noted that nine also had active remote user IDs, and three had privileged access.

   In February 2001, the "Termination Personnel Action Form/Employee Clearance Form," which is the form used when an employee terminates with the City, was revised to include a "Security" section. A department representative is to check the box to indicate that an ISS change order has been submitted to delete system access permissions for a terminated employee. Completion of this section of the form is voluntary, meaning that the checkbox is marked by the department indicating that they have notified ISS that the employee has terminated. Unless specifically noted on the form, a person could have access to other application systems unknown to ISS.

2. User IDs and passwords are being shared among multiple

persons in many end-user departments (examples include: police, fire, treasurer-clerk, electric), as well as in ISS (users with systems administrator privileges). The use of shared user IDs and passwords increases the risk of the password being compromised and undermines the effectiveness of monitoring because individual accountability is lost.

Recently, management revised the HR policy regarding the use of electronic resources (Policy #706.06 J. Electronic Resources and Information Systems) to clarify that employees are to keep their passwords confidential, i.e., should not be shared. If management needs to access resources protected by an employee's password, they can request ISS to reset the password so the resource can be accessed. The Leadership Team was notified of this in July, and all employees were notified in September.

Remote access controls need to be improved to prevent unauthorized persons from obtaining access into the City's network.

During the audit, we noted the following weaknesses related to remote user access.

Weaknesses related to the management of remote access

1. A process is not in place to remove remote access for terminated employees in a timely manner. During our testing, we identified 21 active remote user IDs that belonged to terminated employees.
2. No active monitoring is performed of remote user activities, and the log (two days retained) does not provide a trail should ISS suspect a breach through their call-in lines.
3. Remote user passwords are not adequately protected from disclosure, in that the passwords are accessible

(non-encrypted) to all DNS staff.

4. Strong password controls are not in place for remote access. Specifically, passwords are not required to be periodically changed, and the number of invalid logon attempts is not limited.

Weaknesses related to the management of modems

5. Modems connected throughout the City to individual computers allow a path into the network that bypasses all access controls put in place by ISS. We tested 9,921 of the City's 10,000 designated phone numbers (not all are assigned) after hours only to identify whether an active modem could be detected. We identified 61 modems, and, of those, there were 11 that provided some kind of prompt for user login. Since there are limited, if any, remote access controls on individual computers, the risk is increased that unauthorized persons will be able to obtain access to the City's network via a modem connected to a computer on the network.

Management of password controls needs to be improved to ensure that the controls are in place and operating as intended.

ISS management implemented new password software this past year to enforce aging of passwords (i.e., requiring that they be changed periodically) and limit the number of invalid logon attempts. During our fieldwork, we conducted testing to provide assurances that these newly implemented controls were in place and working effectively.

Weaknesses related to the management of passwords

1. While we noted that the security settings in the password software were in place, we also noted that these settings could be overridden by the security rules in the operating system, thereby nullifying the password software security settings. We found several examples where the intended password software controls were overridden and,

therefore, not in place for City users. The most common override was that passwords were not set to expire instead of being required to be changed every 45 days.

2. A process is not in place at the ISS help desk to verify a caller that requests his/her password be reset. In other words, the helpdesk staff does not verify the authenticity of the caller before resetting the password. Without properly identifying the caller as a current City employee, an unauthorized person could request that a City employee's password be reset and then could obtain access into the network using that employee's user ID and password.

Networks should have adequate controls in place to ensure that unauthorized users do not access the system. Adequate access controls need to address both direct network access as well as remote access paths, including modems. Such network logical access controls include:[11]

- being able to identify individual users or computers that are authorized to access computer networks, data, and resources (i.e., prohibit sharing of user IDs and passwords);
- producing and analyzing audit trails of user activity;
- taking defensive measures against intrusion; and
- having adequate password controls to authenticate users.

Basic password controls include that passwords should: only be known by one person and used to authenticate that person's identity; be of adequate size (not fewer than four characters) defined by the agency; have a maximum lifetime of one year (can be less); be replaced when compromised (suspected or confirmed); be deleted or replaced when a

[11] Federal Information System Controls Audit Manual, Vol. 1 Financial Statement Audits, and Systems Auditability and Control, Module 8, "Telecommunications"

person is no longer an authorized user; be stored in a protected manner so that only the password software can access them.[12]

Management has implemented some operating procedures, but these are not being monitored

While management has implemented some operating procedures addressing user IDs and passwords, adequate measures are not in place to monitor and ensure that the procedures are being followed.

Without adequate user ID and password controls in place for both direct network access and remote network access, the risk is increased that unauthorized persons will access the network and that detection of such a breach will not be detected in a timely manner.

Recommendations related to user access controls, passwords, remote access, and modem management

We recommend that ISS develop and implement adequate user access controls to ensure that only authorized users are able to access the City's network, directly or remotely. Such controls should address a process for obtaining and removing a user ID and password, sharing of user IDs and passwords, minimum password criteria, periodic monitoring to detect unauthorized login attempts in a timely manner, and management and control of the use of modems.

Since ISS has a central modem bank, we also recommend that all dial-up activity be channeled through the ISS Central Modem bank to eliminate the need for analog modems. Should this not be possible, we recommend ISS conduct periodic testing to identify unauthorized modems.

Users with privileged access can add or delete users, make changes to security files, and access every area in the network

Privileged access should be limited to only those areas that users need to perform their job responsibilities.

In the City, there are a number of users with privileged access capabilities that do not appear to be necessary for

[12] Federal Information Processing Standards Publication 112, National Institute of Standards and Technology

their position, i.e., they have been assigned system administrator access. These users can add or delete users, make changes to the security files and settings, and access every area of the network, including operating system, programs, and data stored on the network.

The primary group of privileged users includes application and system programmers, operators, and security administrators. These individuals require certain system or security privileges to perform their job; these privileges include the ability to define or alter security definitions and in some cases allow unrestricted access to data through utilities. Since this group of users requires powerful privileges to perform their jobs, they also have the ability to alter or bypass security controls. (Bypassing security controls can occur through the intentional misuse of powerful utilities or by "hijacking" special authorities.)

Inadvertently, non-ISS staff were assigned privileged access capabilities

During our testing, we also noted that vendors and non-ISS employees were inadvertently assigned privileged access capabilities. And lastly, we noted that there was a lack of segregation of duties in that one of the Business Systems Analysts in the ISS Application Systems section was assigned privileged access capabilities of a system administrator.

Management states that they have assigned this level of responsibility to all those persons they feel need this to perform their job duties. They feel that reducing the number of persons that have this level of access will negatively impact the level of customer service to the City departments.

While customer service is an appropriate objective for ISS, the risk that someone inappropriately accesses confidential data or that inappropriate actions are taken increases directly with the number of persons that have special access levels.

Privilege and control do not have to be mutually exclusive. Privileges can be assigned in a restrictive way and controls implemented to ensure that those privileges are monitored and not abused. Therefore, detective controls such as monitoring security events and status changes are the primary response to potential abuse or the intentional hijacking of special privileges.[13]

Management should limit who is assigned privileged access

We recommend that ISS management limit who is assigned privileged access; privileged users only be assigned individual user IDs, i.e., no sharing; access for vendors be deactivated when they are not currently authorized to be working on the City's systems; and ISS implement periodic monitoring of the activities of these users to ensure that they are only accessing authorized areas and performing authorized transactions.

Protection Of Confidential Data

Confidential data, as defined by Chapter 119.07, Florida Statutes (F.S.) is not being adequately protected in the City's various information systems to prevent improper disclosure.

Chapter 119, F.S., provides for the inspection, examination, and duplication of all public records. There are, however, many exemptions to this statute. Exemptions are "created or maintained only if the exempted record or meeting is of a sensitive, personal nature concerning individuals; the exemption is necessary for the effective and efficient administration of a governmental program; or the exemption affects confidential information concerning an entity."

[13] Handbook of IT Auditing, Price Waterhouse Coopers, 2000 Edition

Examples include:

Exemptions to Chapter 119, "Inspection, examination, and duplication of records"

⇒ Section 119.07(3)(x) states that all employees' social security numbers are exempt.

⇒ Section 119.07(3)(i) identifies specific personal information (address, phone number, social security number, etc.) for certain public positions that are exempt. These include: active and former law enforcement personnel and their spouses and children; revenue collection and enforcement or child support enforcement; active firefighters (certified according to F.S. 633.35); current and former code inspectors and their spouses and children; and directors and managers of human resource departments, labor relations, employee relations, and their spouses and children.

⇒ Section 119.07(3)(b) states that active criminal intelligence stored in the police information is exempt.

⇒ Section 119.07(3)(o) states that data processing software that is sensitive is exempt, including: programs that store data exempt from public record, payroll and control and access authorizations and security measures for automated systems.

In addition, the City receives funding from federal grants that require that specified information be protected from disclosure.[14] Examples include drug testing of transportation workers, medical information of passengers utilizing special transportation services, and testing results for hepatitis B. To comply with these grants, the City must take measures to adequately protect this data.

[14] OMB Circular A-130, Transmittal Memorandum #4, dated 11/28/00, Management of Federal Information Resources

As described in the background section (on pages 10-12), there are various layers of logical access controls that need to be in place to adequately protect programs and data, and these controls are the responsibility of either ISS or the primary business user (i.e., the department-owner). The department-owner is responsible for: knowing what data is stored in the application; specifying the level of application security required for their operations and supporting information systems; and determining who is given access to their application system and what transactions they can perform, such as inquiry only, add, change, and/or delete.

Data has been classified in order to identify data that should be protected

We worked with City departments to identify the types of data that were being stored in City information systems and whether the data was protected by a federal or state law, or local ordinance. Data was classified as public, confidential (exempt from public record), or sensitive. We defined sensitive data as data not protected by law, but which contained the type of information that should not be displayed to everyone. Such sensitive data might include legal information or worker compensation claims.

Listed below are the weaknesses we noted during our testing of security of selected applications that housed or transmitted confidential data. Also, the corrective actions taken in response to weaknesses noted are provided in italics.

Systems contained data not being adequately protected; and status of corrective actions taken

1. Folders/directories belonging to Energy Services and Taltran were not adequately protected from unauthorized users. As a result, it was possible for employees working in another department to read, alter, or destroy files in areas of the network that they shouldn't be able to access. (*Access was immediately corrected to appropriately allow only authorized users. In addition,*

Energy Services management will periodically review who is in their access group.)

2. Terminated employees still had access to certain police application systems. As a result, former employees could possibly read, alter, or destroy data and/or programs in the City's network that they could still access. (*Security Administrators were notified, access was removed as necessary, and the security administrator has implemented a procedure to perform periodic reviews of the user IDs. Police management has also added removal of network and applications user access to their checklist for terminated employees, "Internal Clearance Form." In addition, Fire administrators are implementing a procedure to ensure that the appropriate Police security administrators are notified of terminations in a timely manner.*)

3. User IDs are being shared in certain police application systems. The use of shared user IDs and passwords increases the risk of the password being compromised and undermines the effectiveness of monitoring because individual accountability is lost. *(Police management and security administrators are aware of this and are researching alternative user access methods. In addition, they have developed and implemented internal information security procedures to help mitigate the associated risks.)*

4. Employee information that should have been identified as exempt from public record was not identified as such in the Human Resource Management System. As a result, employee information that should be exempt from public record could be improperly disclosed. *(Management was*

notified and corrections were made. In addition, Human Resource management: (1) sent out guidance (dated July 2001) to City staff regarding how exempt records are marked in the HRMS and the process for handling public records request; (2) provided guidance related to the public records exemptions on the Human Resources Department Intranet web site; and (3) worked with security administrator to further protect this information via queries and reports.)

5. There were different methods of marking an employee as exempt in the Human Resources Management System (in the Human Resources module and the Retirement module), making it possible for someone to inadvertently release exempt information. *(Retirement management was notified and is working with ISS to develop a way to identify all currently affected retirees. Future retirees should be properly identified when the records are transferred from Human Resources to Retirement modules within the system.)*

6. In two application systems (Customer Information System, Energy Loan Database), there is currently not a way to indicate that an employee or customer record should be exempt from public record. As a result, anytime the City completes a request for data from these information systems, personal information that should be exempt from public record could be improperly disclosed. *(Management has been notified. The Customer Information System is currently being replaced, and management has stated that an indicator will be added to the system during implementation. Energy Services management is currently exploring what options are*

available regarding how to best to identify those records that should be exempt in the Energy Loan Database .)

7. E-mail containing confidential information is being transmitted among City employees in an unprotected manner. It is possible that the e-mail could be accessed and read by an unauthorized person. *(ISS is researching the use of encryption software that could be used by any City employee to encrypt e-mail messages and attachments when transmitting confidential information.)*

8. The City's Permit Tracking System (also referred to as PETS) contains personal information about certain City employees that is exempt from public record per Chapter 119, Florida Statutes. Currently, no mechanism is in place to identify these individuals or the information as being confidential. In addition, this information is made available on the City/County Internet site that provides the status of building permits. (*City/County GIS* staff and *Growth Management staff are exploring the methods to mark these records as confidential and removing the personal information from the Internet site. The data is originally obtained via the County Property Appraiser's database; therefore, the county needs to be advised of the need to protect this information within their database also.)*

We consider all of the above issues important enough to warrant immediate management attention. Without proper identification and protection of the confidential data, there is an increased risk that the City may inadvertently and improperly disclose this protected information and defeat the protections intended by state and federal laws.

Recommendations related to protection of confidential data

<u>We recommend</u> that the department-owners determine what

information stored in their applications is exempt from public record by federal or state law, or local ordinance. Department management should request assistance from the City Attorney if they need help to make that determination. Then, we recommend the department-owners establish controls to adequately protect data defined as exempt from public record from unauthorized access and inadvertent disclosure. Department management should request assistance from ISS if they need help establishing computer system access controls.

Conclusion

Inadequate information security is a management problem. Ensuring adequate security requires ongoing attention and monitoring the risks and the effectiveness of mitigating controls. The challenge is for managers to view information security management as an integral element of the City's operations by:

- considering the security implications whenever computer and telecommunications technology is being used to support program operations,
- weighing the potential costs and benefits by determining what level of risk is acceptable in light of the expected cost to address the risk, and
- providing adequate resources to monitor controls and keep risks at a manageable level.

We would like to thank staff from ISS and all the departmental staff that provided their support and assistance during this audit.

ISS and other departmental representatives have been very responsive to correcting user access weaknesses that were identified during the audit. There is a great need for management to implement policies, procedures, standards, and processes toward the prevention, detection, and correction of information security weaknesses.

Management's action plan to address the significant issues identified in this report is presented in Appendix B.

Response from Appointed Officials

City Manager:

We appreciate the thorough review of the logical security of the City's Local Area Network by the City Auditor's Office. We believe the action plans will address all the recommendations in the report and we believe these plans can be implemented by the projected dates shown in the action plans.

Interim City Treasurer-Clerk:

We concur with the recommendations made in the Logical Security Audit as they relate to the Treasurer-Clerk's Office and have implemented the suggested changes.

Copies of this audit report #0201 (project #0101) may be obtained from the City Auditor's web site (http://talgov.com/citytlh/auditing/index.html), by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (dooleym@talgov.com).

Audit conducted by:
Beth Breier, CPA, CISA, Senior IT Auditor
Sam M. McCall, CPA, CIA, CGFM, City Auditor

Appendix A - Methodology

At the start of this audit, management identified those logical access controls that were believed to be in place and those areas that needed improvement. We incorporated the information management provided into our objectives and methodology. During our review of the logical security controls related to the City's LAN, we performed the following audit procedures to achieve our audit objectives.

- To obtain a general understanding of the network operations and logical access paths into the network, we interviewed key personnel in the Information Systems Services and the departments responsible for logical security and City applications, and reviewed ISS network architecture documentation and diagrams.
- To provide assurances and evaluate the adequacy of those logical security controls management believed were in place or should be improved, we: 1) examined password software features and actual settings; and 2) conducted testing to determine how user access is granted and whether user access is removed in a timely manner.
- To determine the adequacy of policies and procedures related to access into the City's LAN, we reviewed relevant Florida Statutes, City ordinances and policies and procedures, and industry practices related to logical security.
- To determine the adequacy of controls in place to prevent unauthorized access into the City's LAN, and determine the accessibility to confidential information stored on the City's LAN, we: 1) surveyed department management to identify those City application systems that house

confidential[15] and/or sensitive information; 2) tested to determine whether access levels for users with special privileged accesses were appropriate; 3) tested to determine whether access to applications and data containing confidential data was properly limited (testing was limited to network level access, not through the application security); and 4) conducted limited testing to identify vulnerable modems, i.e., modems that could provide unauthorized entry points to the City's network.

This audit is limited to the logical security of the City's LAN. Physical security of the City's LAN was addressed in a previous audit ("Physical Security of the City's Local Area Network," Report #0106, issued December 2000).

This audit was conducted in accordance with Generally Accepted Government Auditing Standards.

[15] For purposes of this audit, "Confidential" is defined as being required to be exempt from public record or disclosure per state law, federal law, federal grant requirement, or local ordinances.

Appendix B - Action Plan

Objectives and Action Steps	Responsible Employee	Target Date
A. Objective: ***Develop, obtain approval, and distribute appropriate information security policies and procedures. Educate and train department staff regarding the information security policies and procedures in order to protect the City's computer resources.***		
1. Provide draft security policies to a city employee committee for review and incorporate appropriate feedback into the draft document	Terry Baker	1/11/02
2. Provide draft security policies to City management, including City Attorney's Office, Treasurer-Clerk's Office, Human Resources for feedback and to ensure the proper process is followed	Don DeLoach	3/31/02
3. Present final draft security policies to City management, including Executive Team, Appointed Officials, and other appropriate persons as determined for feedback	Don DeLoach	4/30/02
4. Identify the appropriate City staff to provide training to all City employees as to the security policy detail	Don DeLoach	5/31/02
B. Objective: ***Designate an information security manager(s) to manage and monitor the City's information security policies and procedures. Management has decided to develop an information security group to address the City's information security needs.***		
1. Designate an information security group to consist of various information security related positions, such as: technology infrastructure administrator, database administrator, computer operations and customer service supervisor, and mission-critical application security administrators	Don DeLoach	4/1/02

Objectives and Action Steps	Responsible Employee	Target Date
2. Information security group is to develop standard operating procedures for implementing security activities, such as: coordinating and conducting information security awareness training for employees; routinely monitoring security activities, such as suspected or actual security breaches; recording, tracking, and analyzing suspected and actual information security incidents; and assisting department-owners in assessing the confidentiality and security requirements of their data (also called assessing risks).	Don DeLoach	7/31/02
3. Periodically contract with an outside vendor to assess the City's information security infrastructure.	Don DeLoach	On-going
C. Objective: ***Develop and implement adequate user access controls to ensure that only authorized users are able to access the City's network, directly or remotely, including managing user IDs and passwords, managing use of modems, and monitoring and detecting unauthorized access attempts.***		
1. Develop standard operating procedures in DNS for staff to understand the processes need to be in place regarding how to add, change, transfer, and delete user access. In addition, it will include periodic monitoring procedures to ensure that the controls are in place.	Terry Baker, Joe Kaperak	1/2/02
2. Contract to have a vulnerability assessment of current City network infrastructure performed to identify all potential areas of weaknesses.	Don DeLoach Terry Baker Joe Kaperak	11/30/01
3. Implement recommendations from the vulnerability assessment results	Terry Baker Joe Kaperak	6/30/02
4. Perform post review after implementation of the recommendations	Terry Baker Joe Kaperak	7/30/02
5. Identify and determine the functionality of all modems operating in the City and implement adequate controls to ensure that the network cannot be accessed without proper authentication.	Terry Baker Dale Spivey	1/2/02

Objectives and Action Steps	Responsible Employee	Target Date
D. Objective: ***To adequately protect confidential information by providing security awareness training regarding nondisclosure requirements for information protected by federal or state law, or local ordinance, and establishing controls to protect the data from unauthorized access and inadvertent disclosure.***		
1. Police security administrators need to develop and implement a process to perform periodic reviews of the user IDs in their systems.	Police Technical Services	11/30/01
2. Police Department should examine the use of shared passwords and determine a way to adequately protect their data.	Police Technical Services	11/30/01
3. Fire Department is to develop and implement procedures to inform the CAD/RMS security administrator when employees terminate from the Fire Department.	Tom Cone	11/30/01
4. In HRMS, a consistent use of the "public record" indicator should be implemented, and staff should be notified and trained as needed.	Steve Chase Jean Love	12/31/01
5. Customer Information System (CIS) – a. CIS project team should design and implement a method to identify a customer as being exempt from public record in the new CIS. b. All exempt employees should be identified in the CIS, and staff should be notified and trained regarding how the indicator is to be utilized.	Ted Kinsey	3/31/02
6. Energy Loan Database – Energy Services management is to explore options and implement a process to identify which records are exempt from public record in the database to minimize the risk that personal information for exempt employees is improperly disclosed.	Bob Seaton Jan McCall	3/31/02
7. Research to identify the best encryption software that could be used by any City employee to encrypt e-mail messages and attachments when transmitting confidential information. Roll out the use of the encryption software to those departments with the greatest need and train staff as needed.	Terry Baker	1/2/02

Objectives and Action Steps	Responsible Employee	Target Date
8. Growth Management and City/County GIS - staff need to remove personal information for exempt employees from their Internet site, determine a method for identifying a record as exempt. Steps include: a. A subcommittee of the PETS inter-local steering committee is to identify optional methods to identify records that should be exempt from public records in the PETS systems. b. The PETS inter-local steering committee will evaluate and then select the most cost efficient and least work-intensive option to implement. c. PETS technical staff will design and implement the approved method and develop a process to periodically verify that the records that should be protected are identified as such.	Park Malloy PETS Inter-local Committee	6/1/02

OFFICE OF THE

CITY OF TALLAHASSEE

REPORTING ON
ACCOUNTABILITY
WITH A CITIZEN
FOCUS

CITY AUDITOR