The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver’s government. He also chairs the City’s Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Dennis Gallagher, Chair  Robert Bishop  
Maurice Goodgaine  Jeffrey Hart  
Leslie Mitchell  Timothy O’Brien, Co-Chair  
Rudolfo Payan

Audit Staff

Audrey Donovan, Deputy Director, CIA  
Stephen E. Coury, IT Audit Supervisor, CISA  
Jennifer L. Ware, Lead IT Auditor, CISA  
Ketki Dhamanwala, Senior IT Auditor, CIA, CISA

You can obtain copies of this report by contacting us at:

Office of the Auditor
201 West Colfax Avenue, Department 705 • Denver CO, 80202
(720) 913-5000 • Fax (720) 913-5026

Or download and view an electronic copy by visiting our website at:

www.denvergov.org/auditor
To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people. We will monitor and report on recommendations and progress towards their implementation.
Members of Audit Committee
Ms. Janice Sinden, Chief of Staff
Ms. Stephanie O’Malley, Deputy Chief of Staff
Ms. Cary Kennedy, Chief Financial Officer
Mr. Doug Friednash, City Attorney
Ms. Janna Bergquist, City Council Executive Staff Director
Mr. L. Michael Henry, Staff Director, Board of Ethics
Ms. Beth Machann, Controller
Mr. Ethan Wain, Deputy Chief Information Officer

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people.

We will monitor and report on recommendations and progress towards their implementation.
AUDITOR’S REPORT

We have completed an audit of Network Security Management – Phase 1. As our review is continuing into its second and final phase, there will be another report issued at the audit’s conclusion. The purpose of the audit was to determine whether the City’s data network is protected from unauthorized access and whether controls are effective in protecting network confidentiality, integrity, and availability.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We identified three areas in which the City’s network security can be improved: information security governance, network equipment inventory controls, and equipment maintenance funding allocations. In order to address these deficiencies, Technology Services should establish an information security governance program, to enable remediation of existing security vulnerabilities and help improve future practices through the development of standards and procedures. To ensure success of the program, the Chief Information Officer should ensure the information security governance program has the full support for authority and funding from the Mayor and City Council. Additionally, Technology Services should redesign its network equipment inventory procedures to ensure reliable records of equipment location. Further, Technology Services should establish procedures for allocation of network equipment maintenance funding to ensure that mission-critical equipment is maintained and that scarce resources are not spent on equipment that has been retired or replaced.

We extend our appreciation to the Chief Information Officer and his staff who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CICA
Director of Audit Services
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY**  
Opportunities Exist to Improve Information Security Governance, Network Equipment Inventory Controls, and Maintenance Funding Allocations  

**INTRODUCTION & BACKGROUND**  

**SCOPE**  

**OBJECTIVE**  

**METHODOLOGY**  

**FINDING 1**  
Information Resources Are at Risk Due to a Lack of Information Security Governance  

**RECOMMENDATIONS**  

**FINDING 2**  
Network Equipment Inventory Records Are Inaccurate Due to Missing Controls  

**FINDING 3**  
Network Equipment Maintenance Funding Allocation Procedures Are Not Documented  

**RECOMMENDATION**  

**APPENDICES**  
Appendix A – Executive Order No. 18  
Appendix B – Detailed Site Visit Testing Procedures  
Appendix C – Photos of Conditions Observed  

**AGENCY RESPONSE**
EXECUTIVE SUMMARY

Opportunities Exist to Improve Information Security Governance, Network Equipment Inventory Controls, and Maintenance Funding Allocations

Network security management encompasses the configuration, deployment, and protection of critical City information infrastructure. A vast majority of City services utilize information systems that are interconnected through the City’s large and complex computer network. The City’s network equipment must be protected from unauthorized access to ensure that the network remains available to support City business operations and to ensure that information or equipment is not damaged or stolen.

This report summarizes the first phase of our audit of the City and County of Denver’s network security. Findings in the areas of information security governance, network equipment inventory controls, and equipment maintenance funding allocations are presented along with Management’s responses. As our review is continuing into its second and final phase, there will be another report issued at the audit’s conclusion.

Information Resources Are at Risk Due to a Lack of Information Security Governance

Information security governance is a risk mitigation framework utilized by Information Technology (IT) leadership to develop information security policy with standards and procedures that ensure optimal information security implementations, consistent results, and accurate records. We found a lack of strong leadership and authority for information security governance within the City resulting in weak information security awareness and heightened risks to City information and equipment. Specifically, in almost half of the sites we sampled throughout the City, one or more of the following conditions were present:

- Network equipment is not physically protected from access by the general public
- Network equipment is mounted precariously or not protected from contact with people or objects
- The general public has access to portions of the City’s internal data network

Prior to the City’s consolidation of IT functions into a shared services model in 2004, the City utilized a fragmented system where some City agencies managed their own IT requirements and others maintained their own IT departments. As a result of this disparate structure, some agencies were not aligned with information security management best practices. When the Technology Services Department (Technology

---

1 The audit scope is limited to the portions of the network specifically managed by the Technology Services Department. Refer to the Introduction & Background for additional details.
Services) assumed responsibility for maintaining the City’s network equipment and providing IT support to various agencies, it inherited the existing conditions. Further, Technology Services did not correct security issues. This resulted in the perpetuation of antiquated practices and conditions for more than seven years without risk mitigation.

Without an information security governance program, Technology Services operates without sufficient information security awareness, resulting in equipment being deployed or network segments being implemented without adequate protections. Accordingly, Technology Services should establish an information security governance program, to enable remediation of existing security vulnerabilities and help improve future practices through the development of standards and procedures. To ensure success of the program, the Chief Information Officer should ensure the information security governance program has the full support for authority and funding from the Mayor and City Council.

Network Equipment Inventory Records Are Inaccurate Due to Missing Controls

The City’s network infrastructure is made up of thousands of components. All of this equipment must be maintained in order to keep the network running efficiently and effectively. However, in order to maintain the equipment, Technology Services must have a reliable record of where all the network’s components are housed. When we tested network inventory records for eighteen locations, we identified a 71 percent discrepancy rate between records and equipment found. Specifically, we noted discrepancies in equipment details, items that were recorded in inventory but not present at the location, and items that were present at the location but not recorded in inventory.

We concluded that the inventory records are not reliable. Accordingly, Technology Services should redesign its network equipment inventory procedures and conduct a thorough inventory so that resources spent to secure and protect network assets and to mitigate risks are based on reliable information.

Network Equipment Maintenance Funding Allocation Procedures Are Not Documented

Technology Services spent over $832,000 for network equipment maintenance (warranty support) in 2011. However, the justification and criteria for this spending is not documented. Further, Technology Services personnel make maintenance spending decision on an informal basis rather than on a formal, systematic planning process. The current process lacks transparency and presents a risk to the City in the event of personnel turnover. For example, replacement staff may not be able to make informed decisions about maintenance, potentially resulting in inefficient use of resources. Further,
without accurate inventory records maintenance could be inappropriately spent for retired or replaced equipment. Documenting these procedures will help protect against key personnel turnover and provide transparent criteria for maintenance expenditures.

INTRODUCTION & BACKGROUND

The City and County of Denver’s Data Network

The City and County of Denver operates a large and complex data network that supports the interconnection of computers and other electronic devices used to conduct City business and to provide services to the citizenry. The network connects all City locations where agencies have offices or information technology systems thus enabling business systems, telephones, and email to connect to data centers across town and to the Internet.

City offices with network connections include libraries, recreation centers, police and fire stations, and human services centers. Network connections are also utilized by systems not contained within offices, such as traffic control and video surveillance systems. Some agencies, such as libraries, also provide network connections to enable the public to access the Internet through either a City-provided computer or a wireless connection. Nearly all City agencies depend on the availability of the network to conduct their business and to provide services to the public, thus making the network a critical component of the City’s information infrastructure.

The Technology Services Department (Technology Services) manages a large part, but not all, of this Metropolitan Area Network. Portions of the network are managed by other agencies, such as, the Denver International Airport, Denver District Attorney’s Office, and Denver County Courts. This audit included only the portion of the network managed by Technology Services.

Managers of the City and County of Denver’s Metropolitan Area Network

Network Security Management

The City’s data and network connections must be protected against unauthorized access. Network security management is the discipline that ensures that network

---

Footnote: 2 A Metropolitan Area Network connects offices distributed throughout the area of a large city.
equipment is properly configured, deployed, and protected from unauthorized access, which includes physically protecting network equipment.

Technology Services manages over 270 network equipment locations distributed over the 153 square miles of Denver, resulting in an average of about 1.8 network locations per square mile. Protecting this large number of equipment locations over such a wide geographic area is a significant task. As information security is only as strong as its weakest link, the requirement for strong and consistent information security practices is paramount in order to protect the network from unauthorized access, damage, or theft of equipment.

What is Information Security Governance?

Information security governance is the tone set and the actions taken by the executive management within an IT organization, including the Chief Information Officer, to ensure optimal information security implementations, consistent results, and accurate records.

A Mature Information Security Governance Model

More specifically, information security governance is "... a framework for making appropriate risk mitigation decisions and building the organization’s ability to protect and react to external and internal threats."³

Over time a mature information security governance organization will develop an information security program that includes:

- Communication and reporting to City executive management on the effectiveness and efficiency of the information security governance program according to key performance indicators. Further reporting on security incidents, information security risk trends, and any other information security risk issues that management needs to know.

A standardized risk assessment methodology to address exceptions and provide formal notification to management with a documented and approved assumption of risk when necessary

Business impact analyses

Development of information security policies, standards, and procedures

Design and execution of an employee information security awareness training program

Information security architectural design review and assessment of IT deployments of applications, equipment, and network configuration

Vulnerability and threat analysis

Developing procedures for incident response

Developing standards for disaster recovery and business continuity planning

Remediation strategies and projects

Self-audit and compliance testing

Continuous monitoring to ensure controls are still relevant and functioning as designed

A mature information security governance program features continuous monitoring to ensure compliance with standards. As highlighted in an Industry study by the Ponemon Institute, an independent research center that conducts studies on privacy, data protection and information security policy, it is by far more cost effective to comply with security practices than it is to recover from security problems. “On average, non-compliance cost is 2.65 times the cost of compliance....”

Responsibility for Information Security Governance

According to Executive Order No. 18, the responsibility for “Ensuring that City information technology systems, data, and networks are secure and available to the City’s internal and external customers” is placed within Technology Services. The agency is managed by the Chief Information Officer who is appointed by the Mayor. Please see “Appendix A – Executive Order No. 18” to view the entire Executive Order.

---


SCOPE

The audit focused on segments of the City and County of Denver’s Metropolitan Area Network that are managed by Technology Services, which excludes the portions of the network that are managed by other agencies, such as, the Denver International Airport, Denver District Attorney’s Office, and Denver County Courts.

This report summarizes the first phase of our audit. As the review has a subsequent phase, a final and separate report will be issued at the audit’s conclusion.

In accordance with Generally Accepted Government Auditing Standards (GAGAS) the reader should be aware that some details about information security weaknesses are considered sensitive security information and are not disclosed within this report.

The details of all findings, however, have been presented to the City’s Chief Information Officer. The City’s Audit Committee will also receive a briefing during an executive session. As part of our regular follow-up for audit issues, we will return at a future date to ensure that all findings have been addressed.

OBJECTIVE

The purpose of the audit was to determine whether the City’s data network is protected from unauthorized access and whether controls are effective in protecting network confidentiality, integrity, and availability.

METHODOLOGY

We utilized several methodologies to achieve the audit objectives. Please see “Appendix B – Detailed Site Visit Testing Procedures” for more detail about the testing techniques and tools used during our site visits. Our evidence gathering techniques included, but were not limited to:

- Examining policies, standards, and procedures for maintaining inventory records
- Evaluating controls around the inventory management process
- Selecting a sample of network equipment sites in order to:
  - Interview Technology Services personnel, field technicians, and agency personnel
  - Conduct a physical review of network inventory to determine accuracy and completeness of inventory records
  - Test publicly accessible network ports to determine whether the data network was open to unauthorized users
○ Conduct walkthroughs to scan for and detect unauthorized wireless access points
○ Observe physical security, equipment protection, and environmental controls around network equipment
• Consulting best practice standards such as National Institute of Standards and Technology (NIST) publications, Institute of Internal Auditors (IIA) publications, and the Federal Information System Controls Audit Manual (FISCAM)
• Reviewing audits conducted by other organizations
FINDING 1

Information Resources Are at Risk Due to a Lack of Information Security Governance

Information security governance is “... a framework for making appropriate risk mitigation decisions and building the organization’s ability to protect and react to external and internal threats.”\(^6\) We found conditions indicating that the City has weak information security awareness and is lacking strong leadership and authority for information security governance.

As an illustration of this issue, for almost half of the eighteen sites we sampled throughout the City, we identified one or more of the following conditions:

- Network equipment is not physically protected from access by the general public
- Network equipment is mounted precariously or not protected from contact with people or objects
- The general public has inappropriate access to portions of the City’s internal data network

Additionally, we found the following conditions that inhibit the ability to ensure the confidentiality, integrity, and availability of City business systems:

- Network equipment is installed in environmentally harsh conditions without temperature monitoring or regulation, and subject to adverse and extreme temperature ranges
- Audible alarms signaling temperatures out of tolerance within equipment rooms are not monitored
- Computers are installed with access to sensitive networks in areas allowing direct physical access to hardware by prisoners incarcerated by the City and County of Denver
- Prisoners are allowed physical access to alter computer configuration settings
- Prisoners are allowed to make unauthorized access attempts to the Internet which results in continuous system maintenance and configuration corrections
- Areas where network equipment is received, tested, and configured are open to the general public
- Network monitoring software is accessible by any internal user
- Wireless access points are not installed for optimal performance

- Wireless networks not supported by Technology Services are operating on City premises
- Computers with wireless capability are allowed to connect and broadcast on ad hoc or peer-to-peer networks
- Unprotected network cabling is installed through a non-city controlled area
- Equipment is installed in areas not easily accessible for maintenance and support
- Training user IDs and passwords are posted in public areas
- Training user IDs have e-mail accounts

In addition to the physical conditions observed, we noted that Technology Services does not provide a Citywide information security awareness training program. Some of the conditions observed may not have existed if such training had taken place.

Both the nature and the number of conditions found are alarming considering we only tested approximately 6 percent of the street addresses where network equipment is located and as information security is only as strong as its weakest link. See “Appendix C – Photos of Conditions Observed” for photos of some of the conditions observed.

Prior to the City’s consolidation of IT functions into a shared services model in 2004, the City utilized a fragmented system where some City agencies managed their own IT requirements and others maintained their own IT departments. As a result of this disparate structure, some agencies were not aligned with information security management best practices. When Technology Services assumed responsibility for maintaining the City’s network equipment and providing IT support to various agencies, it inherited the existing conditions. Further, Technology Services did not correct security issues. This resulted in the perpetuation of antiquated practices and conditions for more than seven years without risk mitigation.

The absence of an overall information security governance program results in the deployment of equipment or network segments without adequate protections. The establishment of an information security governance program can enable remediation of existing security vulnerabilities and help improve future information security practices through the development and enforcement of policies, standards, and procedures.
RECOMMENDATIONS

The Auditor’s Office offers the following recommendations to ensure the security of the City’s information resources:

1.1. The Chief Information Officer should establish an information security governance program with the authority to define policy and enforce standards and procedures across City agencies.

1.2. The Chief Information Officer should ensure the information security governance program has the full support for authority and funding from the Mayor and City Council.

1.3. The Technology Services Department should establish an information security governance program that is led by a person independent of operational responsibility so that the function can remain focused on directing solutions for protecting the City’s information assets and network infrastructure. The components of the program should include:

- Communication and reporting to City executive management on the effectiveness and efficiency of the information security governance program according to key performance indicators. Further reporting on security incidents, information security risk trends, and any other information security risk issues that management needs to know.

- A standardized risk assessment methodology to address exceptions and provide formal notification to management with a documented and approved assumption of risk when necessary.

- Business impact analyses

- Development of information security polices, standards, and procedures

- Design and execution of an employee information security awareness training program

- Information security architectural design review and assessment of IT deployments of applications, equipment, and network configuration

- Vulnerability and threat analysis

- Developing procedures for incident response

- Developing standards for disaster recovery and business continuity planning

- Remediation strategies and projects

- Self-audit and compliance testing

- Continuous monitoring to ensure controls are still relevant and functioning as designed
FINDING 2

Network Equipment Inventory Records Are Inaccurate Due to Missing Controls

The City’s network infrastructure consists of thousands of components. All of this equipment must be maintained in order to keep the network running efficiently and effectively. However, in order to maintain the equipment, Technology Services must have a reliable record of where all the network’s components are housed. Tests of network inventory records for eighteen locations identified the absence of basic inventory controls as demonstrated by a 71 percent discrepancy rate. Errors were of three types: discrepancies in equipment description within the inventory records; items existing in inventory records but not found at the location; and items found at the location but not listed in inventory records. Refer to Table 1 for the error rate per discrepancy.

Table 1 - Discrepancy Error Rates

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrepancies in equipment description within the inventory records</td>
<td>13%</td>
</tr>
<tr>
<td>Items existing in inventory records but not found at the location</td>
<td>65%</td>
</tr>
<tr>
<td>Items found at the location but not listed in inventory records</td>
<td>22%</td>
</tr>
</tbody>
</table>

We performed a two-way test of inventory records by comparing inventory records to what we found at equipment facilities (known as “book-to-floor” testing) and by comparing what we found at the facility to the inventory records (also known as “floor-to-book” testing).

Technology Services maintains the network equipment inventory on a Microsoft Excel spreadsheet stored on a network shared drive. Although it is password protected, the password is commonly known by Technology Services personnel. Further, the spreadsheet is maintained by multiple persons who update it when new equipment is installed and when equipment is moved or taken out of service. There are no inventory change tickets or transactions that can be used to verify that necessary changes are made, which also prevents supervisors from being able to perform a review for completeness and accuracy (i.e. an audit trail). The equipment inventory is not

---

7 The 71 percent represents the number of discrepancies from our control records adjusted for differences encountered during the site walkthrough.
periodically verified with what is actually installed in the field, so many errors go undetected.

Our review of the network inventory record-keeping procedures identified four areas where controls were deficient or missing. First, there is no segregation of duties for people who have both access to equipment assets and update responsibility for inventory records. Second, there is no accountability for access to the spreadsheet, and access is only controlled through a commonly known password. Third, there are no transaction records for changes to inventory. The absence of an audit trail does not enable people to check their own work. Further, a supervisor cannot review the completeness of work performed. Fourth, there is no periodic verification that the inventory records match what is installed in the field, thus preventing the detection of missing equipment or errors in the inventory records.

Due to the high error rate and lack of controls, we concluded that the inventory records are not reliable. Technology Services is the custodian of network assets and must maintain accurate records. Further, accurate records are essential for ensuring that scarce resources allocated to purchase and protect network assets is based on reliable information. Without an accurate inventory listing of equipment in use and its location, Technology Services could be hindered in meeting its goal of effectively managing and maintaining the City’s network infrastructure and components. In order for field technicians to maintain and service equipment, they need to accurately identify its location. Accordingly, Technology Services should redesign its network equipment inventory procedures to adopt specific controls including segregation of duties, accountability for access, inventory change transaction records, and periodic inventory verification.
RECOMMENDATION

The Auditor’s Office offers the following recommendations to ensure that network equipment inventory records are accurate:

2.1. The Technology Services Department should redesign its network equipment inventory procedures to enhance controls in four areas:

a. Segregation of duties should be enforced to ensure that those with physical access to equipment are not responsible for updating inventory records.

b. Access to the network equipment inventory should be restricted to a minimum number of people. File share permissions should be used to restrict access and the spreadsheet password should be eliminated.

c. A procedural checklist or some other type of transaction record should be devised to support documenting changes made to the spreadsheet. These transaction records can be used by both the people updating the records and their supervisors to ensure that all transactions are recorded accurately. The transaction records along with periodic copies of the spreadsheet should be archived for historical use.

d. After the preceding controls are established and tested for reliability, the entire network equipment inventory should be field verified to ensure its accuracy. This can be accomplished in phases over a period of time, perhaps up to a year. Once, the entire inventory has been reconciled, only subsequent sampling of sites should be required to ensure the process is maintaining accurate records.
FINDING 3

Network Equipment Maintenance Funding Allocation Procedures Are Not Documented

Allocation of funding for network equipment maintenance (warranty support) should be based on a comprehensive, documented spending plan so that year-to-year maintenance contract renewal costs can be effectively and strategically evaluated. In 2011, Technology Services spent over $832,000 for network equipment maintenance (warranty support).

Technology Services generally purchases maintenance contracts for new equipment and reviews those contracts annually. Currently, personnel who are familiar with the equipment and its history make subjective decisions regarding which equipment should still be included in the annual extension of the maintenance contract. However, the criteria for these decisions are not documented in a formal procedure and there is no assessment of the cost-benefit of maintenance spending decisions.

In the event of personnel turnover, replacement staff will not be able to make informed decisions about what maintenance to renew, potentially resulting in inefficient use of resources. Further, the absence of a formal spending plan is exacerbated by inaccurate inventory records (as noted in the prior finding). As a result of this condition, scarce maintenance funds could be inappropriately spent on retired or replaced equipment. Accordingly, Technology Services should formalize its equipment maintenance funding allocation procedure.

RECOMMENDATION

The Auditor’s Office offers the following recommendations to ensure that network equipment maintenance procedures are documented:

3.1. The Technology Services Department should design a procedure for allocating funding for network equipment maintenance to ensure that efficient allocations continue to occur in the event of personnel turnover. The procedure should identify how to determine which equipment should be included, how to determine if equipment has reached end of life, and under what circumstances maintenance should be terminated.
APPENDICES

Appendix A – Executive Order No. 18

EXECUTIVE ORDER NO. 18

TO: All Agencies Under the Mayor

FROM: John W. Hickenlooper

DATE: June 17, 2005

SUBJECT: Establishment of Technology Services and Definition of its Mission and Functions

Purpose: This Executive Order shall establish Technology Services and define its mission and functions. Executive Order No. 18, dated March 19, 1999, is hereby cancelled and superseded by this Executive Order.

1.0 Applicable Authority: The applicable authority relevant to the provisions and requirements of this Executive Order No. 18 is found in Section(s) 2.2.1, 2.2.6, 2.2.8, 2.2.10, and 2.9.3 of the Revised Charter.

2.0 Establishment of Technology Services: Technology Services and its divisions are already established. The agency oversees the technology service delivery functions of the City government, utilizing best practices uniformly on all technology development and operations, and improving service performance. The agency is managed by the Chief Information Officer who is appointed by the Mayor. The Chief Information Officer may organize the City's various technology operations as necessary to deliver the most effective service. The primary responsibilities of the agency are:

2.1 Developing and supporting integrated software solutions, data management and system quality assurance.

2.2 Ensuring that City information technology systems, data, and networks are secure and available to the City's internal and external customers.

2.3 Reviewing and approving all technology purchases made by the City.

2.4 Ensuring that new and established Technology Services products and services are delivered on time and within approved budgets.

2.5 Providing electronically delivered information and transactional business capabilities to public constituents and internal customers.

3.0 Mission: The mission of Technology Services is to provide superior customer service, communication, and tools, through the effective use of applied technology to help our users and the City as a whole meet business objectives.
Executive Order No. 18
Page two

4.0 **Functional Cooperation with the Office of Telecommunications**: An additional function of Technology Services is to cooperate with the Office of Telecommunications in matters related to the oversight of the City and County of Denver’s cable television franchise.

5.0 **Memorandum Attachments**: The procedures for implementing this Executive Order may be defined by Memorandum Attachments to the Executive Order, which shall become a part of the Executive Order. Further, the Chief Information Officer shall have the authority to issue procedural Memorandum Attachments relative to this Executive Order.
Appendix A – Executive Order No. 18 – (Continued)

Executive Order No. 18
Page three

Approved for Legality:

Cole fires
City Attorney for the City and County
Of Denver

Approved

John W. Hickenlooper
MAYOR

Vicki Braunagel
Co-Manager of Aviation

Terry West
Co-Manager of Aviation

Nancy Stevenson
Manager of Environmental Health

Luis A. Colon
Manager of General Services

Kim Bailey
Manager of Parks & Recreation

Bill Vidal
Manager of Public Works

Cheryl D. Cohen-Vade
Manager of Revenue

Kevin J. LaCasse Jr.
Manager of Safety

Roxanne White
Manager of Human Services

Peter Park
Director of Planning & Development
Appendix B – Detailed Site Visit Testing Procedures

Sample Selection

Using the official network equipment inventory records maintained by the Technology Services, we selected a testing sample of eighteen sites where network equipment is housed. The variety of sites selected were:

- Representative of City business
- Representative of a diversity of agencies and facilities
- Potentially less controlled in order to identify possible “weakest links”
- Geographically dispersed throughout the City

Figure 1 shows the approximate locations of the sites tested.

*Figure 1 - Map Showing Locations of Sites Tested*
Appendix B – Detailed Site Visit Testing Procedures – (Continued)

Summary of Site Types

The types of sites selected for testing included a variety of categories, such as recreation centers, fire stations, and more. Table 2 provides a summary of the types of sites selected for testing.

Table 2 - Classification of Sites Tested

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Sites Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>1</td>
</tr>
<tr>
<td>City Council</td>
<td>1</td>
</tr>
<tr>
<td>Concessions</td>
<td>1</td>
</tr>
<tr>
<td>Courts &amp; Detention Facilities</td>
<td>1</td>
</tr>
<tr>
<td>Event Venue</td>
<td>1</td>
</tr>
<tr>
<td>Fire Stations</td>
<td>2</td>
</tr>
<tr>
<td>Golf Course</td>
<td>1</td>
</tr>
<tr>
<td>Human Services</td>
<td>1</td>
</tr>
<tr>
<td>Libraries</td>
<td>1</td>
</tr>
<tr>
<td>Network Hub</td>
<td>1</td>
</tr>
<tr>
<td>Police Facilities</td>
<td>3</td>
</tr>
<tr>
<td>Public Works</td>
<td>1</td>
</tr>
<tr>
<td>Recreation Centers</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18</strong></td>
</tr>
</tbody>
</table>

Details of Tests Performed

**Physical and Environmental Security:** The audit team conducted a physical and environmental security walkthrough of each testing location to review the following conditions:

- Access to the network equipment is restricted
- Access to the network equipment is limited
- Network equipment is securely mounted
- Network equipment is housed in an area with little human traffic
- Network equipment is not exposed to excessive sunlight, wind, dust, water, or other elements
- The temperature and humidity levels surrounding the network equipment are appropriate
Each site was ranked according to two vectors: one for physical security and the other for the protection of equipment within the facility. Each vector ranked the condition at high, medium, or low to indicate the level of risk to the equipment. The definitions for high, medium, and low were slightly scaled back from the highest standards found in best practices so that they would be considered more practical and reasonable for the City’s environment.

Table 3 shows that nearly half the sites ranked high in risk for either physical security of the facility or for protection of equipment within the facility.

### Table 3 - Site Risk Summary

<table>
<thead>
<tr>
<th>Physical Security</th>
<th>Equipment Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>18</td>
<td>18</td>
</tr>
</tbody>
</table>

Note: The names of the sites corresponding to the numbers above are intentionally omitted for security reasons.

**Port Configuration Verification:** We conducted a walkthrough of each location to identify network ports that were available to the public. A netbook computer equipped with a network cable was used to determine if discovered ports were active. If an active port was found, additional testing was conducted to determine if the port was configured to allow access to the Internet only, the internal City network, or both. When access to the internal City network was allowed, testing was conducted to further identify if shared folders or other important applications could be accessed.
Rogue Wireless Access Point Discovery: The audit team used an InSSIDer® Wi-Fi network scanner running on a netbook computer and an iNet® application running on smart mobile phones and tablet computers to conduct a walkthrough of each location, as well as the surrounding areas, to identify wireless access points. Access points that were determined to be associated with the location (and not with the surrounding facilities) were vetted with Technology Services to determine if they were supported or rogue access points. Similar to the port configuration verification, additional testing was conducted on identified wireless networks to determine if access was granted to the Internet only, the internal City network, or both.

If an access point was identified with weak or no encryption methods, we made an attempt to access the network equipment using vendor default IDs and passwords; however, we did not use brute force password hacking or other persistent techniques.

Field Verification of Inventory: The network equipment for each location was identified according to the master inventory spreadsheet maintained by Technology Services. During the site visit, we conducted a walkthrough to physically verify, via serial number, if the equipment noted on the master inventory spreadsheet was deployed at the location (known as “book-to-floor” testing).

When we identified network equipment at a location that was not recorded in the master inventory spreadsheet, we noted the serial number and model. We then conducted further research using the spreadsheet and Technology Services’ personnel (also known as “floor-to-book” testing).

---

8 InSSIDer is a Wi-Fi network scanner developed by MetaGeek, LLC. The software was downloaded on the netbook so that Wi-Fi scans could be conducted during the site visits

9 iNet is a mobile device WiFi scanner developed by Banana Glue. The software was downloaded to the mobile devices so that the network address of devices could be revealed once access was gained to the wireless network. This enabled further testing of the wireless access point’s security settings.
Appendix B – Detailed Site Visit Testing Procedures – (Continued)

Tools Used

Figure 2 illustrates the tools used by the audit team to conduct site testing:

- Netbook computer running inSSIDer software for scanning Wi-Fi networks and equipped with a network cable for testing wired connections
- Smart mobile phones and a tablet computer running network scanning applications (iNet)
- Portable infrared digital thermometer to measure focused ambient (wall) temperature
- Portable digital thermometer and humidity meter
- Digital camera

**Figure 2 - The Network Auditor’s Toolkit**
Appendix C – Photos of Conditions Observed

The following photos (Figures 3 through 8) illustrate some of the conditions observed during testing. For security reasons, their locations are not disclosed.

Figure 3 - Equipment mounted precariously - Velcro strapped to shelf

Figure 4 - Equipment not protected from people or objects - liquid spray bottle placed on equipment

Figure 5 - Equipment mounted precariously - placed on heater - not protected from people or objects - chair can come into contact with equipment

Figure 6 - Equipment mounted precariously – not protected from people or objects

Figure 7 - Door to equipment room found open and has no lock

Figure 8 - Equipment mounted precariously – Velcro strapped to shelf
March 2, 2012

Mr. Kip R. Memmott, MA, CGAP
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Department 705
Denver, CO 80202

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Network Security Management (Phase 1).

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report draft that was sent to us on February 9, 2012. This response complies with Section 20-276 (b) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1: Information Resources Are at Risk Due to a Lack of Information Security Governance

RECOMMENDATION 1.1: The Chief Information Officer should establish an information security governance program with the authority to define policy and enforce standards and procedures across City agencies.

<table>
<thead>
<tr>
<th>RECOMMENDATION 1.1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree or Disagree with Recommendation</td>
<td>Target date to complete implementation activities (Generally expected within 60 to 90 days)</td>
<td>Name and phone number of specific point of contact for implementation</td>
</tr>
<tr>
<td>Agree</td>
<td>October 15, 2012</td>
<td>Chuck Fredrick 720-913-4906</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1:
Agency agrees with the recommendation. The establishment of an information security governance program will begin immediately with assessing and assembling current documents into a central location. The next step will be to identify the shortcomings and lay out a strategy for completing or updating any documents.

In addition, the Agency believes the ability to execute and sustain an effective governance program will be dependent on additional information security governance resources, as recommended by your office below in Recommendation 1.2. Adequate resources for Information Security Governance will be requested by the Chief Information Officer as part of the 2013 budgeting process. Results of the 2013 budget process should be finalized no later than October of 2012.

RECOMMENDATION 1.2: The Chief Information Officer should ensure the information security governance program has the full support for authority and funding from the Mayor and City Council.
### RECOMMENDATION 1.2

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 15, 2012</td>
<td>Chuck Fredrick 720-913-4906</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.2:**
Agency agrees with the recommendation. The Chief Information Officer will advocate for full support of this program, balanced with careful consideration of the City’s projected financial situation for 2013. A sustainable governance program will be developed based on available funding in 2013.

### RECOMMENDATION 1.3

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 15, 2012</td>
<td>Patrick Klein 720-913-4875</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.3:**
Agency agrees with the recommendation. As stated in the previous two recommendations, the gaps in the existing information governance program can be determined with existing information security resources (note: at time of completion of this letter, not all positions are filled). Technology Services will advocate for additional resources required to implement this function independent of operational duties, as part of the 2013 budget process. A sustainable governance program will be developed based on available funding in 2013. Results of the 2013 budget process should be finalized no later than October of 2012.
AUDIT FINDING 2: Network Equipment Inventory Records Are Inaccurate Due to Missing Controls

RECOMMENDATION 2.1: The Technology Services Department should redesign its network equipment inventory procedures to enhance controls in four areas:
   a. Segregation of duties should be enforced to ensure that those with physical access to equipment are not responsible for updating inventory records.
   b. Access to the network equipment inventory should be restricted to a minimum number of people. File share permissions should be used to restrict access and the spreadsheet password should be eliminated.
   c. A procedural checklist or some other type of transaction record should be devised to support documenting changes made to the spreadsheet. These transaction records can be used by both the people updating the records and their supervisors to ensure that all transactions are recorded accurately. The transaction records along with periodic copies of the spreadsheet should be archived for historical use.
   d. After the preceding controls are established and tested for reliability, the entire network equipment inventory should be field verified to ensure its accuracy. This can be accomplished in phases over a period of time, perhaps up to a year. Once, the entire inventory has been reconciled, only subsequent sampling of sites should be required to ensure the process is maintaining accurate records.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>March 15, 2013</td>
<td>Patrick Klein 720-913-4875</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 2.1: 
Agency agrees with the recommendation. The agency will review the job duties of the current employees as well as the procedures for receipt and documentation of inventory. Where possible we will develop procedures to reduce or eliminate any conflict of interest. The separation of duties will require an additional full-time position, which will be requested as part of the 2013 budget process as described above.

Regarding the inventory, we will review the procedure to improve the documentation and tracking to include the possible procurement of an asset management application. Once the documentation process is defined, we will conduct a full inventory of network assets. Due to the number of locations and amount of equipment to be inventoried, this process will take twelve months to complete.

AUDIT FINDING 3: Network Equipment Maintenance Funding Allocation Procedures Are Not Documented

RECOMMENDATION 3.1: The Technology Services Department should design a procedure for allocating funding for network equipment maintenance to ensure that efficient allocations continue to occur in the event of personnel turnover. The procedure should identify how to determine which equipment should be included, how to determine if equipment has reached end of life, and under what circumstances maintenance should be terminated.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>September 15, 2012</td>
<td>Patrick Klein 720-913-4875</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 3.1:
Agency agrees with the recommendation. The agency will review the current process and develop a single source of truth on assets. With this process will be included a methodology on the maintenance to be applied to each type of equipment/license. We will reconcile the information with the service provider annually to verify assets are properly covered. The next cycle for maintenance ends in June 30 2012, which will be our goal for completion of the first phase. A second phase will be conducted once a complete inventory is finished, which we intend to complete by September 15, 2012.

Please contact Patrick Klein at 720-913-4875 with any questions.

Sincerely,

[Signature]
Chuck Fredrick
Chief Information Officer

cc:   Ethan Wain, DCIO
      Pat Klein, Network and Telecommunications Director
      Ravi Kumar, Director, Enterprise Architecture