Industrial Control Systems
Performance Audit

May 2015

Office of the Auditor
Audit Services Division
City and County of Denver

Dennis J. Gallagher
Auditor
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
- Maurice Goodgaine
- Leslie Mitchell
- Rudolfo Payan
- Robert Bishop
- Jeffrey Hart
- Timothy O’Brien, Vice-Chair

Audit Management

- Kip Memmott, Director, MA, CGAP, CRMA
- John Carlson, Deputy Director, JD, MBA, CIA, CGAP, CRMA
- Audrey Donovan, Deputy Director, CIA, CGAP, CRMA

Audit Staff

- Shannon Kuhn, IT Audit Supervisor, CISA
- Nicholas Jimroglou, Lead IT Auditor, CISA
- Jakki Boline, Senior IT Auditor
- Karin Doughty, Senior IT Auditor, 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) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
A2014-020
Dear Mr. Daidone, Ms. Benavidez, Mr. Cornejo, and Ms. Dannemiller:

Attached is the Auditor's Office Audit Services Division's report of its audit of Industrial Control Systems (ICS). The purpose of the audit was to identify ICS applications in use throughout the City and determine the extent to which stakeholders are prepared to address and assess cyber risks and overall security measures in place for these applications that are owned and managed by the City.

The audit found that governance over the administration of ICS applications is not formalized by Technology Services management and provided to agencies to reduce risk to industrial systems that are responsible for the operations of key areas or are critical to the City's infrastructure.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5000.

Sincerely,

Dennis J. Gallagher
Auditor

cc: Honorable Michael Hancock, Mayor
    Honorable Members of City Council
    Members of Audit Committee
    Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
    Ms. Janice Sinden, Chief of Staff
    Mr. David P. Edinger, Chief Performance Officer
    Ms. Beth Machann, Controller
    Mr. Scott Martinez, City Attorney
    Ms. Janna Young, City Council Executive Staff Director
    Mr. L. Michael Henry, Staff Director, Board of Ethics

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 Industrial Control Systems (ICS) operations and security infrastructure. The purpose of the audit was to examine ICS application security controls to determine the extent to which the systems are managed by appropriate procedures. We also assessed whether hardware and software security measures have been implemented correctly, are operating as intended, and are producing the desired outcomes.

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.

The audit found that Technology Services management does not provide guidance to agencies that operate ICS applications, which would reduce risks and promote compliance for all computing devices and address system security measures. Additionally, some agencies responsible for the day-to-day operations of ICS applications manage these systems with limited guidance and knowledge of security best practices.

We extend our appreciation to the teams, technicians, and personnel of the Departments of Public Works, General Services, Parks and Recreation, and Technology Services who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CRMA
Director of Audit Services
Industrial Control Systems Performance Audit
May 2015

The audit examined the cyber risks and security counter measures for Industrial Control Systems (ICS) that operate and monitor key City resources such as traffic signals, internal building controls, and public amenities.

**Background**

Industrial Control Systems (ICS) are computer-based systems used to automate industrial equipment that was initially operated through a mechanical device or manual process. For example, the City uses ICS applications to monitor and adjust building temperature, regulate ventilation, control traffic lights, and manage irrigation systems and swimming pools.

**Purpose**

The purpose of this audit was to assess the City’s internal control environment related to ICS applications to determine areas of vulnerability. We reviewed roles and responsibilities for the management and configuration of ICS applications to determine if guidance was provided by Technology Services subject matter experts on industrial system security measures to assist the agencies and departments with managing their ICS applications.

**Highlights**

The audit found that the City does not have a governance strategy to manage the use of Industrial Control Systems (ICS) and has not assessed ICS applications for security and operational integrity. This was apparent in both the high-level governance of these systems as well as the day-to-day operations of some of the City's ICS applications. From a governance perspective, we found that Technology Services is not providing guidance to agencies with regard to how ICS applications should be properly secured against information security threats. Administrators of these systems, most of whom do not have an information technology background, would greatly benefit from guidance provided by subject-matter experts in Technology Services. This would also ensure that ICS applications are protected in a consistent way across the City.

From an operational perspective, we identified information security risks associated with the management of ICS applications that are connected to the City's traffic light system; some that help automate certain building systems, such as heating and cooling; and those that regulate Department of Parks and Recreation irrigation systems and swimming pools. These systems are not being administered in accordance with City information security policies and industry best practices, placing the City at risk of inappropriate access, sabotage, system malfunction, inefficient use of resources, and customer dissatisfaction.

For a complete copy of this report, visit www.denvergov.org/auditor
Or Contact the Auditor’s Office at 720.913.5000
# TABLE OF CONTENTS

## INTRODUCTION & BACKGROUND
- Introduction to Industrial Control Systems 1
- Industrial Control Systems Used by the City 2
- Risks to Industrial Control Systems 5

## SCOPE
7

## OBJECTIVE
7

## METHODOLOGY
8

## FINDING
9
- The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity 9

## RECOMMENDATIONS
16

## AGENCY RESPONSE
18
INTRODUCTION & BACKGROUND

Introduction to Industrial Control Systems

Federal, state, and local infrastructure such as electrical plants, oil and gas pipelines, heating, ventilation, and air conditioning (HVAC) units, dams, and sewage treatment plants are important to the safety and well-being of citizens in our society. Many of these systems were initially designed to be operated manually or mechanically without automation in mind. This required such things as the manual manipulation of water valves, powering on and off HVAC units, and controlling gas pressure.

Industrial Control Systems (ICS) are computer-based systems used to automate industrial equipment that was initially performed through a mechanical device or manual process. There are several different types of ICS applications, such as Building Automation Systems (BAS) that automatically monitor and adjust building temperature, regulate ventilation, maintain and manage water pressure, control lighting, and send alert notifications when environmental factors are outside tolerable ranges. An ICS applied to an irrigation system assists in scheduling watering times, controls flow rates, and helps operate within governmentally implemented water restrictions. An ICS applied to a public pool automatically dispenses precise levels of chlorine, monitors water flow rates and temperature, and alerts personnel when levels are unsafe. Figure 1 shows several systems an ICS can control.

Figure 1: Types of Systems Controlled by Industrial Control Systems

Source: Created by Audit Services Division staff.
A larger scale ICS is known as a supervisory control and data acquisition (SCADA) system. These are used to control systems that are part of an underlying infrastructure such as water treatment, wastewater, oil and gas, and electrical power. The City does not manage any SCADA systems.

Using an ICS reduces the need to perform manual tasks to manage important infrastructure systems, which are labor and time intensive. For example, at the end of the business day, facilities management personnel would be responsible for walking through an entire building, turning off lights and lowering thermostats to save energy. An ICS performs all these tasks automatically, as well as re-illuminating the building in the morning, adjusting the temperature, and even generating daily reports on building conditions. Although an ICS efficiently and effectively controls equipment, it cannot replace human judgment in the event of malfunction or failure. Additionally, personnel are still needed to maintain, monitor, and manage an ICS.

Industrial Control Systems Used by the City

Various ICS applications are used to manage City public services and infrastructure. In 2004 the City’s Technology Services department (Technology Services) adopted a shared service model, which consolidated technology staff from most agencies into a single technologies department responsible for overseeing computing resources for the City, with the exception of Denver International Airport, Denver Public Library, and Denver County Courts. Despite this shift from a decentralized to a centralized approach, many ICS applications are not supported by Technology Services.

**Building Automation Systems** - Twenty-six City buildings are controlled by BAS systems, including the City and County Building, which is home to the Mayor’s office, Civil Courts, meeting facilities for City Council, the Office of Emergency Services, and myriad other important City functions. These buildings have several BAS applications that manage functions such as temperature, ventilation, and indoor and outdoor lighting. Thirteen Department of Parks and Recreation (Parks and Recreation) BAS applications control City-owned public facilities, such as the Martin Luther King and Washington Park Recreation Centers, which are heavily used.

**Department of Parks and Recreation** - Parks and Recreation also uses an ICS to irrigate the public golf courses, public City parks, and street medians. There are approximately 240 City parks, 28 recreation centers, and 7 golf courses owned and operated by the City as shown in Figure 2. An estimated 31 million gallons of water were used in 2014 to irrigate the Wellshire golf course alone. An ICS helps Parks and Recreation regulate water use during Denver’s hot summer months to ensure healthy grass while also conserving water.
Parks and Recreation also use an ICS to dispense chemicals into swimming pools to keep them safe and clean for public use. The City has sixteen outdoor swimming pools and thirteen indoor swimming pools, managed by products from a single vendor. These products provide pool technicians a way to remotely monitor pool conditions from a workstation located within the aquatics office. Figure 3 shows a popular swimming destination and its associated ICS equipment.
Although parks, golf courses, and swimming pools are heavily used by Denver citizens, the ICS with the greatest visibility and daily impact is the traffic management system.

Traffic Management - Denver was the second United States city to install an electric traffic signal, which was first used in 1923. Today, the City’s Department of Public Works (Public Works) manages nearly 1,200 traffic signals, including miles of fiber optic cables. Prior to the use of central systems, traffic signals ran independently of each other and there were no alarms; monitoring and remote programming were not available. Figure 4 shows an example of the type of electromechanical dials that were previously used to control traffic lights.

The City moved from the manual manipulation of signals to an ICS. It is important to secure ICS-managed devices in such a way that they are isolated from the Internet to prevent access from cyber attacks. The City’s current ICS traffic system is used to monitor intersections and configure traffic signals. The same traffic system application is used by the Colorado Department of Transportation and

**Figure 3: Parks and Recreation Swimming Pools**

Right – A Swimming Pool Industrial Control System and Automatic Dispenser

Below – Popular City Pool (Photo from www.denvergov.com)

**Figure 4: Older Traffic Dials**

Source: http://www.trafficsignalmuseum.com/
neighboring municipalities, so Denver’s traffic patterns can easily be coordinated with neighboring communities. Figure 5 shows the City’s traffic monitoring station.

**Figure 5:** The City’s Traffic Management Center

![Traffic Monitoring Station](image)

*Source:* Created by Audit Services Division staff.

### Risks to Industrial Control Systems

There are risks associated with moving labor intensive industrial operations to an automated system. Many of these systems were originally designed with little or no security controls in place. ICS applications are increasingly connected to other information system networks or the Internet to allow operators to perform tasks remotely. Security vulnerabilities to the systems are increased when they are managed with inadequate security controls in place and exposed to publicly facing Internet connections.

According to the SANS Institute, a security training company, nearly 700 respondents in industries such as healthcare, transportation, oil and gas, and chemical production consider their systems to be at high or severe risk of a security threat. The problem is that when control systems are connected to the Internet or mobile devices, this exposes them to risk against which they were never designed to protect.\(^1\) Equally as important as securing systems is having a governing organization that has a complete listing of all systems in place and has assessed them for risks related to cybersecurity and internal secure systems.

---

threats. It is critical that ICS applications are configured and managed with security controls in place. Some of the effects of ICS outages or failures are damaged reputation due to unavailability of public amenities, traffic jams, lost revenue, and uncomfortable working conditions, which can lead to health issues.

An ICS used to operate systems can be convenient, efficient, accurate, and effective and can improve safety and reduce labor. In the event of a failure, most systems can still be manually controlled, for example, by turning on and off thermostats, boilers, and air conditioners; directing traffic; manually watering parks; and measuring, testing, and applying chemicals to swimming pools.

**Federal ICS Guidance** - Based on these risks and the complex nature of the technology supporting ICS applications, IT functions are the appropriate authority to ensure proper information security governance. The federal government asserts that local jurisdictions are responsible for securing their technology infrastructures. Specifically, the U.S. Department of Homeland Security (DHS) created the National Infrastructure Protection Plan (NIPP) to provide state, local, and tribal governments with a unified and comprehensive approach to securing and managing key resources and critical infrastructure under their jurisdiction. The plan advises these governments to be aware of all technologies that manage key and critical resources and identify risk associated with the systems to ensure that they are secure and free from vulnerabilities.²

In its December 2014 report on federal facility cybersecurity, the U.S. Government Accountability Office (GAO) recommended that DHS develop and implement a strategy to address cyber risk to building and access control systems. Their audit determined that DHS lacks a strategy that defines the problem, identified the appropriate roles and responsibilities, analyzed the resources needed, and identified a methodology for assessing cyber risk. Furthermore, GAO found that DHS has not incorporated cyber threats to building and access control systems in its Design-Basis Threat report that identifies numerous undesirable events.³

---


SCOPE

This audit focused on Citywide Industrial Control Systems (ICS) that control both employee and public spaces such as Building Automation Systems, traffic signals, golf and park irrigation systems, and swimming pools, which are managed and maintained by staff within the agency that houses and is responsible for the management of the devices. We selected a sample of ICS applications based on a combination of risk and public importance. The following ICS applications were reviewed for this audit:

- Department of Public Works, Transportation Division
  - Traffic Light System
- Department of Parks and Recreation
  - Golf Irrigation ICS Applications – Kennedy and Wellshire
  - Park Irrigation ICS Applications – City Park and Washington Park
  - Swimming Pool ICS Applications – Martin Luther King and Central Park
  - Recreation Center Building Automation Systems – Washington Park and Central Park
- Department of General Services, Facilities Management Division
  - Building Automation Systems
    - City and County of Denver Building
    - Wellington Webb Municipal Building
    - A City data center
    - Denver Crime Laboratory
    - Van Cise-Simonet Detention Center

OBJECTIVE

The audit assessed the City’s internal control environment related to technology systems, specifically Industrial Control Systems (ICS). We assessed whether the ICS applications supporting the City provide reasonable assurance that systems are reliable and secure and are performing as intended.

METHODOLOGY

We tested the effectiveness of the security and operational management of Industrial Control Systems (ICS) and selected sample systems that are in use for the Department of Public Works Transportation Division, the Department of General Services Facilities Management Division, and the Department of Parks and Recreation. To assess risks associated with ICS applications, we used a variety of audit methodologies, including:

- Using data analytics and system-generated lists from human resources and facilities to assess physical and logical access to building automation, traffic management, irrigation, and aquatics systems
- Capturing and evaluating ICS configuration including user access and security, password settings, and alarm conditions and notifications
- Obtaining and reviewing relevant Technical Service Agreements, maintenance logs, and work orders
- Reviewing operations manuals and guides for industrial control applications
- Conducting site visits and interviewing agencies responsible for the day-to-day operations of ICS applications to determine what steps they have taken to protect the physical and logical access of these systems
- Researching best practices, frameworks, and standards for ICS policies and procedures from sources including:
  - Federal Information Processing Standards (FIPS) Publication 200
  - Federal Information System Controls Audit Manual (FISCAM) February 2009
  - National Institute of Standards and Technology (NIST) SP 800-82 Guide to Industrial Control Systems (ICS) Security
- Reviewing City Geographic Information System maps and attribute tables and City and County of Denver 2014 Mayor’s Budget to obtain an overview of agencies to be included in the audit
- Reviewing existing Technology Services policies and procedures related to network security and acceptable use of City networks and computing resources
- Interviewing the City’s Information Security Manager to discuss security guidelines for ICS systems, and implementation of security policy at the desktop level
- Interviewing ICS authorized service providers and ICS technical staff to obtain additional information about security measures and secure implementation
- Testing a sample of the City’s ICS applications to verify that they are not public facing
FINDING

The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity

In assessing potential vulnerabilities of the City’s Industrial Control System (ICS) applications, we found issues both with the high-level governance of these systems as well as more specific issues with some of the ICS applications themselves. From a governance perspective, we found that the City’s Technology Services department (Technology Services) is not providing guidance to agencies across the City with regard to how ICS applications should be properly secured against information security threats. Although the day-to-day operations of the majority of ICS applications across the City are the responsibility of the agencies, with the exception of the traffic system, they are being managed by personnel who do not have information technology (IT) backgrounds or skill-sets. Despite strong efforts to secure their ICS applications, these employees would greatly benefit from guidance provided by the City’s information security subject-matter experts in Technology Services, who have knowledge of information security best practices.

From an operational perspective, we identified three areas where ICS applications are being used across the City that have not been safely configured to properly control access: the City’s traffic light system, various Building Automation Systems (BAS) in buildings across the City managed by the Department of General Services (General Services), and ICS applications being managed by the Department of Parks and Recreation (Parks and Recreation). These systems are not being administered in accordance with City information security policies and industry best practices, which places the City at risk of inappropriate access, sabotage, system malfunction, inefficient use of resources, and customer dissatisfaction.

Technology Services Has Not Provided Guidelines to City ICS Operators To Properly Secure ICS Applications

As a result of the audit, we determined that Citywide ICS applications are not being managed at a high level with a global perspective that benefits from the City’s existing information security governance knowledge base. For example, the City does not have a comprehensive inventory of the ICS applications that are in use by various agencies. In order to have an effective governance strategy, the City must identify the total population of systems that need to be secured and managed. Technology Services is the appropriate City agency to maintain an inventory of City ICS applications and provide technical guidance to users.
City agencies with ICS applications use a variety of BAS applications and architectures, all of which must be assessed to identify their unique security vulnerabilities and threats. For example, a BAS application that is managed on a standalone workstation without internet or intranet access has a different set of risks than a system that allows for remote access by ICS operators. Technology Services has not provided security training or guidelines to ICS operators to assist with properly securing the systems and providing continuity in the event of an outage or failure. We found that some of the ICS operators demonstrate information security awareness and recognize the need to implement security measures to address risk; however, they have indicated that they need greater assistance in determining what actions are feasible and appropriate.

The City's Network Administration policy states that workstations should automatically lock after a specified period of inactivity. However, this policy has not been enforced Citywide and thus there are workstations used to manage ICS applications that do not lock when unattended. It should be noted that some of these workstations should be excluded from this policy, such as Denver Sheriff Department systems that are used to display live feeds of inmates and Traffic Management Center monitoring screens that are used to display live feeds of major intersections.

The lack of appropriate ICS management guidelines could result in a system being accessed by unauthorized users, which could cause a system failure or outage. Accordingly, Technology Services should identify and evaluate ICS applications in use throughout the City by establishing a comprehensive inventory and risk assessment, including exceptions to the Network Administration policy. Technology Services should then develop and distribute security guidelines to agencies to assist in the management and administration of ICS applications, taking into account the limitations of these systems. Additionally, Technology Services should identify workstations operating Industrial Control Systems that should not be subject to the IT security lockout provision within the IT security policy.

Systems Owned and Operated by the City are not Securely Configured to Control Access

In addition to identifying weaknesses with the City’s governance of Citywide ICS applications, we found that certain systems may pose an information security threat. Most significantly, this risk was apparent in the management of the City’s traffic light system, but was also evident with various BAS applications and Parks and Recreation ICS applications. Despite these weaknesses, ICS applications were configured to prevent access from the Internet, which is one of the biggest areas open to exploitation by cyber criminals.
The City’s Traffic Light System Is Not Administered In Accordance with Technology Services Security Policies and Procedures or with Security Best Practices

Public Works administers the City’s traffic management system and voluntarily complies with Technology Services security and network policies, even though Technology Services does not have administrative responsibility for the traffic management system. We identified six areas where controls over the traffic management system could be strengthened to improve overall system and application security.

Password Configuration Settings Are Weak

We reviewed security configuration settings on the traffic management system and found that passwords can be re-used more often than is allowed by the City’s Acceptable Use policy. Additionally, password expiration is not enforced by the system, and accounts are not disabled after a number of invalid access attempts as required by the City’s Acceptable Use policy.

This situation exists because the Traffic Management System Administrator inherited the traffic network many years ago and never evaluated existing accounts and security configuration settings. Weak password controls potentially allow unauthorized individuals to repeatedly attempt system access to discover passwords that are not periodically changed. Once an account is compromised by an unauthorized individual, unauthorized changes made to the traffic management system could result in disruptions in routing intersection alerts and configuring intersections. Accordingly, the Traffic Management System Administrator should implement password security settings as established by the City’s Acceptable Use policy.

Badge Access to the Traffic Management Center and Server Room Is Excessive

Although only two or three Public Works employees typically work in the City’s Traffic Management Center (TMC) at any given time, audit work found that nearly three hundred individuals have access to the TMC and seventy-five individuals have access to the server room inside the TMC. The Federal Information Security Controls Audit Manual (FISCAM) recommends adequate security at entrances and exits to facilities housing significant technology equipment, such as this location. Access to facilities should be limited to personnel having a legitimate need for access to perform their duties.

This situation exists because Traffic management has not implemented periodic entitlement reviews of access to the TMC. Weak physical access controls to the TMC could result in loss or damage to traffic systems and data. If the traffic management system is damaged, intersection monitoring and automated alerts could be disrupted, resulting in slower response times to address traffic light errors and anomalies. We recommend that Traffic Engineering Management perform quarterly physical access reviews of the TMC and inner server room.
Traffic Engineering Management Has Not Formalized the Backup and Contingency Planning Process

Although backup servers are in place and an off-site backup location is planned, formal backup and contingency plans have not been documented and distributed. This situation exists because Transportation Management has not made a priority of documenting critical traffic system components and processes, and Technology Services has not communicated the importance of backup and contingency plans related to ICS.

The National Institute of Standards and Technology (NIST) recommends that organizations develop, document, and disseminate contingency plans to affected parties. Lack of a documented and implemented disaster recovery and business continuity plan can result in prolonged down time and the inability to access the traffic management system in the event of a disaster or critical system failure. Transportation Management should develop, document, and implement formal backup and contingency plans for the traffic signal system.

An Excessive Number of Accounts Have Privileged Access to the Traffic Management System

Forty percent of accounts on the traffic management system have privileged access, enabling users to make significant system changes without approval. Additionally, two terminated employees retained access to the system. This situation exists because the system administrator inherited the traffic management system many years ago and has never performed an entitlement review of accounts. Further, Traffic Engineering Management was not aware of information security best practices and has not implemented an IT governance program to provide on-going management of information and network security related to the traffic management system.

Retaining accounts with no business need increases the potential for unauthorized individuals to obtain privileged access to the system, using those accounts to disrupt intersection and alert monitoring. The Federal Information Security Controls Audit Manual recommends that security managers periodically review access authorizations for continuing appropriateness. The Traffic Management System Administrator should perform periodic user access reviews of the traffic signal system and all associated systems.

A Shared User ID and Password Is Used for the Traffic Management System

Audit work found that the traffic management system is accessed using a shared user ID, which is generic, has a shared password, and the password is never changed. This occurred because the traffic management system is currently in the User Acceptance

---

4 National Institute of Standards and Technology, Publication 800-53.

Shared accounts increase the likelihood that an unauthorized user can gain access to the system. Additionally, when accounts are shared and passwords are never changed, transferred or terminated employees would retain the access to the system using that shared account. The City’s Acceptable Use policy requires users to practice adequate password management by keeping all passwords confidential. It also requires passwords to expire every ninety days. Once the system moves out of the User Acceptance Testing phase and into the production environment, the systems administrator should create unique user IDs and require strong passwords to access the system, in accordance with the City’s Acceptable Use policy.

**Traffic Management Has Not Designed, Documented, and Implemented a Change Control Process to Monitor Changes Made by the Vendor**

The traffic management system is in the User Acceptance Testing phase and Traffic Management has not designed, documented, and implemented a change control process to address changes made by the vendor once the system is in production. This occurred because Traffic Management was not aware of standards and best practices requiring monitoring, testing, and approval of vendor software changes prior to implementation on City computing resources.

Unauthorized changes to traffic management system software can result in disruptions to traffic light monitoring and maintaining configurations. FISCAM recommends that an effective change management process be developed, documented, and implemented. Once the system moves out of the User Acceptance Testing phase and into the production environment, the Systems Administrator should ensure that a change management process is instituted, in accordance with the City’s Change Management policy.

**Building Automation Systems Managed by the Department of General Services Are Decentralized and Not Administered Using Security Best Practices**

General Services administers twenty-six BAS systems in City buildings using a variety of different platforms and architectures. We inspected five systems and found that these decentralized systems are not managed using security best practices. The staff managing and using the systems are not receiving security training or being informed of potential vulnerabilities.

**Logical Access Control Practices**

Audit work identified issues with logical access control practices, which specify that individual user accounts and passwords should be instituted when supported by the application or system. This would ensure that system updates and changes are attributed to a specific user. In addition the system administrator should review access on a periodic basis to ensure that access is still appropriate. Accounts for employees who transferred to other positions or are no longer employed by the City should be disabled.
or removed. Finally, in the event that individual user accounts are locked, emergency accounts should be secured until needed.

We found two active unused generic accounts in BAS systems, as well as an active account for a former employee, which could result in unauthorized system access and updates to the BAS systems. We also found instances of staff using a shared account password instead of individual user accounts and passwords, and a shared emergency account and password. When system changes are made with a shared ID and password, there is no individual accountability for the changes made to a system. If an unauthorized change was detected, it would be difficult to ascertain the individual who made the change. The weak logical controls we identified are a result of a lack of security training and security policies specific for BAS application management. Accordingly, the Facilities Director should ensure that Facilities teams perform periodic logical access reviews for their respective BAS systems and require that individual user accounts and passwords be created when supported by a BAS system.

**Backup and Storage Practices**

Backup and storage practices are another element of information security best practices. Providing for regular system backups and secure storage of backups ensures that a system can be restored more quickly in the event of failure. If the system is an ICS that could mean restoring environmental controls such as heating or air conditioning.

During the audit we found a system backup that was stored adjacent to the workstation running the system. If the workstation were to be compromised, the backup could also be damaged by the same event, or in the event of malicious action, the backup could be removed or destroyed. In either scenario the loss of the system and backup could result in downtime and require a time-intensive effort to recreate the system configurations. We identified an additional facility that does have offsite storage of the backup, located with the vendor that performed the initial installation. Although the vendor has provided satisfactory service to the City on an ad-hoc basis, the City does not have a service level agreement (SLA) or technical service agreement (TSA) with the vendor that would provide assurance that they would respond in a timely manner if the backup was needed. We found that there were no policies and procedures that specified frequency of backups or security and storage of the backups.

Accordingly, the Facilities Director should consider obtaining TSAs with relevant vendors to ensure a timely response if a backup copy of the system is needed to restore a BAS system. Additionally, the Facilities Director should request a backup copy that can be stored in a separate location from the workstation.

**Backups of the Parks and Recreation Building Automation Systems and Irrigation Systems at City Parks Are Not Stored Off-site and Backups Do Not Occur Regularly**

When assessing City locations managed by Parks and Recreation, we found issues related to backup procedures for BAS systems as well as ICS applications used to manage irrigation systems. We also found that the Parks and Recreation Facilities team is using shared generic accounts to manage ICS applications.
Backup Procedures

Regularly scheduled backups are important to provide a quick and effective means of restoring system settings. If backups are not created at regular intervals the stored backup may not reflect the current settings within the system and could result in additional time configuring the system. It is also important to store these backups at a different location. If the backup is stored at the same facility where the ICS computer is located and a disaster occurred, both the backup and computer would be lost. This would result in personnel required to manually control the buildings and irrigate the parks.

We reviewed BAS systems at two of the City’s recreation centers and the irrigation systems at two City parks. For the two recreation centers, we found that both the facilities team and the vendor had a backup of the systems that could be used to restore the system, but the backups are not scheduled to occur with any specified frequency. For the two City parks, we found that backups are not performed on a regular basis and are not stored offsite.

This condition occurred because a formal backup policy was never established. Accordingly, the Director of Parks and Recreation should ensure that backups of the agency’s BAS systems and ICS applications managing their irrigation systems are performed periodically and stored offsite.

Shared Generic Accounts

During the audit, we noted that the Parks and Recreation Facilities team is using shared generic accounts to manage the ICS applications. This occurred because Parks and Recreation Facilities team members have not received system security training or been provided guidelines.

When team members use a shared account there is a lack of accountability; system changes cannot be attributed to an individual user. During a walk-through we conducted with Parks and Recreation Facilities personnel, team members gained an understanding of the risks associated with ICS applications and indicated that they are looking for guidance and best practices regarding backups and user access. Accordingly, the Director of Parks and Recreation should ensure that individual user accounts are created for system access.
RECOMMENDATIONS

Technology Services

1.1 Technology Services should identify and evaluate Industrial Control Systems in use throughout the City, which would result in a comprehensive inventory and risk assessment.

1.2 Technology Services should develop and distribute security guidelines to agencies to assist in the management and administration of Industrial Control Systems, taking into account the limitations of these systems.

1.3 Technology Services should identify workstations operating Industrial Control Systems that should not be subject to the IT security lockout provision within the Network Administration policy.

Transportation

1.4 The Traffic Management System Administrator should implement password security settings as established by the City’s Acceptable Use policy.

1.5 Traffic Engineering Management should perform quarterly physical access reviews of the Traffic Management Center and inner server room.

1.6 Traffic Engineering Management should develop, document, and implement formal backup and contingency plans for the traffic signal system.

1.7 The Traffic Management System Administrator should perform periodic user access reviews of the traffic signal system and all associated systems.

1.8 Traffic Engineering Management should monitor vendor access to ensure changes to software are formally requested, approved, and monitored.

General Services – Building Automation Systems

1.9 The Director of Facilities should ensure that Facilities teams perform periodic logical access reviews for their respective Building Automation Systems (BAS) and require that individual user accounts and passwords be created when supported by a BAS system.

1.10 The Director of Facilities should ensure that a backup of each Building Automation System is stored in a location that is separate from the workstation where the Industrial Control System is installed.

1.11 The Director of Facilities should ensure the City has a backup copy of the Building Automation Systems, or as an alternative obtain a formal agreement
from the vendor to ensure a timely response if a backup copy of the system is needed.

Parks and Recreation – Building Automation Systems and Irrigation

1.12 The Director of Parks and Recreation should ensure that backups of irrigation systems and facilities Building Automation Systems are performed periodically and are stored offsite.

1.13 The Director of Parks and Recreation should ensure that teams perform periodic logical access reviews for the Industrial Control Systems they manage.
May 8, 2015

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

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Industrial Control Systems.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on April 17, 2015. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity

RECOMMENDATION 1.1
Technology Services should identify and evaluate Industrial Control Systems in use throughout the City, which would result in a comprehensive inventory and risk assessment.

<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>July 29, 2016</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1
The Governance, Risk and Compliance team in Technology Services will include Industrial Control Systems in a risk assessment process, which will result in a comprehensive inventory for agencies supported by Technology Services.
RECOMMENDATION 1.2
Technology Services should develop and distribute security guidelines to agencies to assist in the management and administration of Industrial Control Systems, taking into account the limitations of these systems.

<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>July 29, 2016</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.2
Technology Services will develop and distribute security guidelines for Industrial Control Systems as part of an updated Information Security Policy.

RECOMMENDATION 1.3
Technology Services should identify workstations operating Industrial Control Systems that should not be subject to the IT security lockout provision within the Network Administration policy.

<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>July 29, 2016</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.3
The Governance, Risk and Compliance team while implementing the Industrial Control Systems risk assessment process, will allow for lockout exceptions to Information Security Policy.
Please contact Alena Gouveia at 720-913-4964 with any questions.

Sincerely,

Frank Daidone
Chief Information Officer

cc:
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
Ms. Janice Sinden, Chief of Staff
Ms. Beth Machann, Controller
Ms. Audrey Donovan, City Auditor’s Office
Ms. Shannon Kuhn, City Auditor’s Office
Ms. Jacqueline Boline, City Auditor’s Office
Mr. Nicholas Jimroglou, City Auditor’s Office
Ms. Karin Doughty, City Auditor’s Office
Mr. Stephen E. Coury, Chief Information Security Officer
Mr. Alena Gouveia, Manager of IT Governance
May 8, 2015

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

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Industrial Control Systems.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on April 17, 2015. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity

<table>
<thead>
<tr>
<th>RECOMMENDATION 1.4</th>
<th>The Traffic Management System Administrator should implement password security settings as established by the City’s Acceptable Use policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agree or Disagree with Recommendation</strong></td>
<td><strong>Target date to complete implementation activities (Generally expected within 60 to 90 days)</strong></td>
</tr>
</tbody>
</table>
| Agree | Completed | Wayne Bobo
720.981.31755 |

**Narrative for Recommendation 1.4**
Password security settings as established by the City’s Acceptable Use Policy have been incorporated into the icons domain TMC network.
**RECOMMENDATION 1.5**

Traffic Engineering Management should perform quarterly physical access reviews to the Traffic Management Center and inner server room.

<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>Completed</td>
<td>Michael Finochio 720.913.0801</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.5**

Access control into the Traffic Management Center (TMC) rooms have been reviewed and updated; moving forward quarterly reviews are scheduled.

**RECOMMENDATION 1.6**

Traffic Engineering Management should develop, document, and implement formal backup and contingency plans for the traffic signal system.

<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>By end of 2015</td>
<td>Michael Finochio 720.913.0801</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.6**

Transportation will generate ongoing implementation and documentation to reflect the traffic signal system backup and contingency plans that are currently in development.

**RECOMMENDATION 1.7**

The Traffic Management System Administrator should perform periodic user access reviews of the traffic signal system and all associated systems.

<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>Completed</td>
<td>Wayne Bobo 720.913.1755</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.7**

Icons domain user access has been reviewed and updated. Transportation will schedule periodic (bi-annual) user access reviews.
RECOMMENDATION 1.8
Traffic Engineering Management should monitor vendor access to ensure changes to software are formally requested, approved, and monitored.

<table>
<thead>
<tr>
<th></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>By End of 2015</td>
<td>Wayne Bobo 720.981.3175 &amp; Michael Finochio 720.913.0801</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.8
Transportation will work with vendors to generate, implement and monitor change management procedures.

Please contact Crissy Fanganello at 720.865.3026 or her designated staff with any questions or clarifications.

Sincerely,

Jose Cornejo, Executive Director
Denver Public Works

cc: Lesley Thomas
Crissy Fanganello
Steve Hersey
Wayne Bobo
Michael Finochio
May 8, 2015

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

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Industrial Control Systems.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on April 17, 2015. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1  
The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity.

<table>
<thead>
<tr>
<th>RECOMMENDATION 1.9</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Director of Facilities should ensure that Facilities teams perform periodic logical access reviews for their respective Building Automation Systems (BAS) and require that individual user accounts and passwords be created when supported by a BAS system.</td>
<td></td>
</tr>
</tbody>
</table>

<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>Aug 6, 2015</td>
<td>James Williamson 720-865-7510</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.9

FM is in agreement with the recommendation.
RECOMMENDATION 1.10
The Director of Facilities should ensure that a backup of each Building Automation System is stored in a location that is separate from the workstation where the Industrial Control System is installed.

<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>Aug 6, 2015</td>
<td>James Williamson 720-865-7510</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.10
GSFM agrees with the recommendation.

RECOMMENDATION 1.11
The Director of Facilities should ensure the City has a backup copy of the Building Automation Systems, or as an alternative obtain a formal agreement from the vendor to ensure a timely response if a backup copy of the system is needed.

<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>Aug 6, 2015</td>
<td>James Williamson</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.11
FM agrees with the recommendation.

Please contact James Williamson at 720-865-7510 with any questions.

Sincerely,

Kevin O’Neil
Facilities Administrative Officer
For:
James E. Williamson
Director of Facilities

cc: Adrienne Benavidez
May 04, 2015

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

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Industrial Control Systems.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on April 17, 2015. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity

RECOMMENDATION 1.12
The Director of Parks and Recreation should ensure that backups of irrigation systems and facilities Building Automation Systems are performed periodically and are stored offsite.

<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>BAS – Agree</td>
<td>05/15/2015</td>
<td>Vernon Paiz 720-865-0380</td>
</tr>
<tr>
<td>Irrigation – Agree</td>
<td>04/30/2015</td>
<td>Debrah Binard 303-806-9084</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 1.12

We agree with this recommendation

Re: Parks & Recreation Building Automation Systems

Denver Parks and Recreation has 12 BAS building temperature controls systems; six of them are web based and 6 are PC software based. Since the ICS audit, we have been working with Trane Company and Tech Services to replace the 6 software based PCs with new Windows 7 desktop units and upgrade the BAS version software. Along with the upgrades we have downloaded software backups with Trane at the PC and will complete our offsite flash drive back up for all 12 systems by 4/30/15. We will use the INFOR preventive maintenance work order system to schedule routine BAS version backups and upgrades. We will also work with Technology Services on the specific protocol to follow.

Re: Parks & Recreation Automated Irrigation Systems

At the time the audit was conducted, the situation regarding central control of Parks irrigation systems was as described in the report. Since then, we have moved central control operation to a virtual terminal server, Toro Sentinel Server (govsenwms01p). The virtual server is maintained and backed up by staff at Technology Services.

Backups are performed nightly and automatically. We perform daily incremental backups at 7:15 pm and run a full back up every two weeks. There are two copies of the backups. One is stored at the Wellington Webb Building and the other at Technology Services location at 10 Galapago. The backups are retained for 30 days, and the first full backup of the month is kept for one year.

### RECOMMENDATION 1.13

<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>BAS - Agree</td>
<td>05/15/2015</td>
<td>Vernon Paiz 720-865-0380</td>
</tr>
<tr>
<td>Irrigation - Agree</td>
<td>4/30/2015</td>
<td>Debrah Bunard 303-806-9084</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.13

We agree with this recommendation

Re: Parks and Recreation Building Automated Systems
BAS password security has been discussed with the ICS audit staff, The Trane Company, and our HVAC staff to create a security plan. All shared password accounts have been inactivated on all the PC systems and will continue with the web based systems. With the web based systems, the manufactures password is imbedded in the system and we may need them to change the programmer password. We will work with Technology Services to develop a security plan that meets the IT Acceptable Use Policies and Procedures guidelines.

A Security Outcome has been added to all appropriate employees PEP’s for 2015 that addresses BAS passwords. The outcome is as follows:

Building Automated Systems
“User shall keep all passwords confidential, shall keep all passwords physically secure and not place a written list of passwords in plain view or anywhere easily discoverable (for example, posted under a computer keyboard or desk drawer) Shall not disclose system passwords to anyone without supervisor approval. Shall not leave any logged into the network device unattended.”

Re: Parks and Recreation Irrigation Automated Systems

The security issues regarding log-ins are resolved. All shared password accounts have been inactivated.

Please contact Fred Weiss at 720-913-0735 with any questions.

Sincerely,

Fred Weiss
Director of Finance and Administration

cc:  Abby McNeal
     Sid Schwarz
     Vernon Paiz
     Debra Binard
     Melvin Thompson
     Lauri Dannemiller