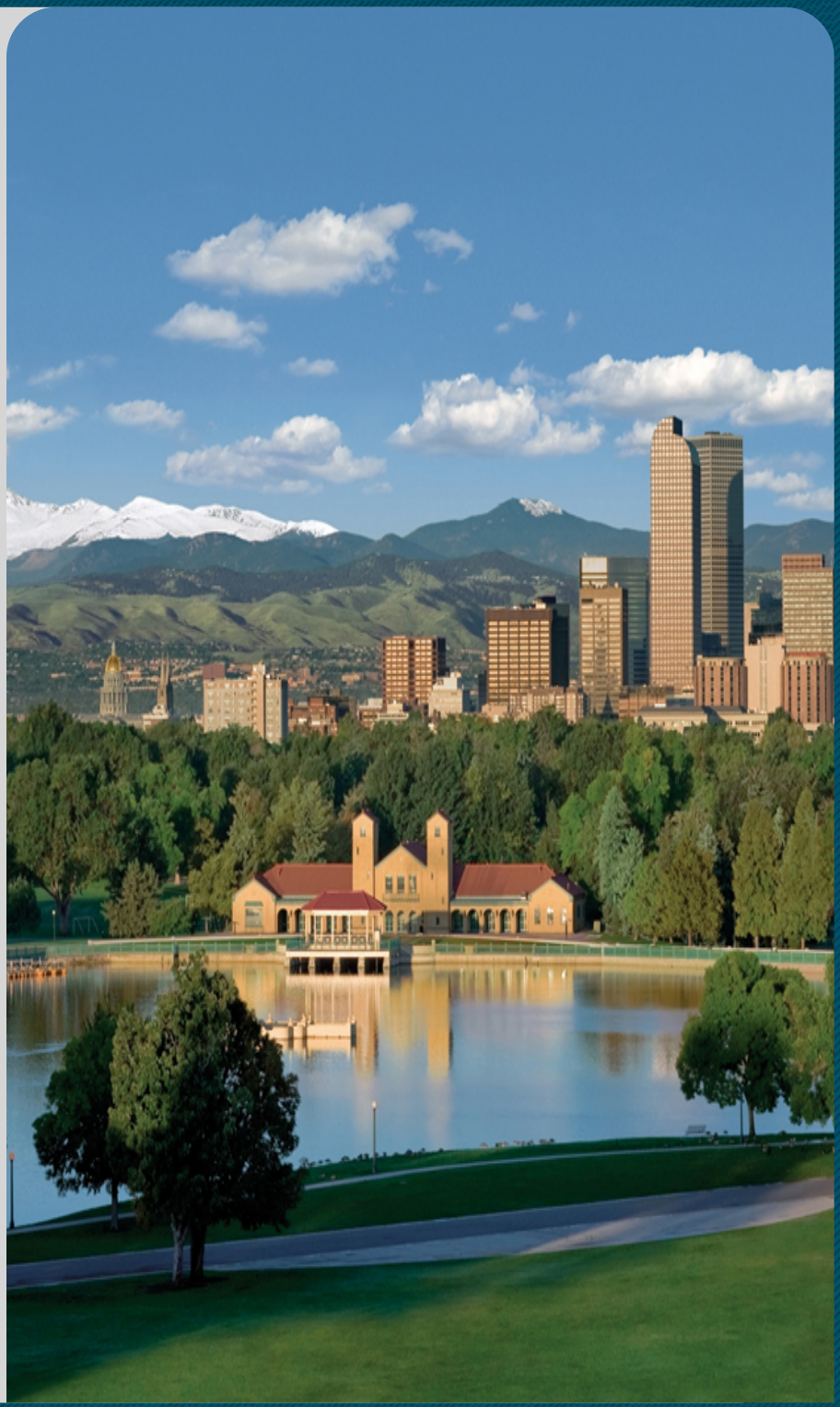
FOLLOW-UP REPORT

Industrial Control Systems Audit

February 2017



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

Timothy M. O'Brien, CPA
Denver 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 and contractors 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.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability 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

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits

Audit Staff

Shannon Kuhn, CISA, IT Audit Supervisor
Nick Jimroglou, CISA, Lead IT Auditor
Karin Doughty, CISA, Senior IT Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #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
Report number: **A2014-020**

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

February 2, 2017

Mr. Scott Cardenas, Chief Information Officer, Technology Services
Mr. Jose Cornejo, Executive Director, Department of Public Works
Mr. Fred Weiss, Financial Director, Department of Parks and Recreation
Mr. James Williamson, Director of Facilities Management, Department of General Services
City and County of Denver

Re: Audit Follow-Up Report

Dear Messrs. Cardenas, Cornejo, Weiss, and Williamson:

In keeping with generally accepted government auditing standards and the Audit Services Division's policy, as authorized by D.R.M.C. § 20-276, our Division has a responsibility to monitor and follow-up on audit recommendations to ensure audit findings are being addressed through appropriate corrective action and to aid us in planning future audits.

This report is to inform you that we have completed our follow-up effort for the Industrial Control Systems audit issued May 21, 2015, which made thirteen recommendations to four City agencies. Our review determined that the General Services and Parks and Recreation departments have adequately implemented all recommendations made to them in the audit report. Technology Services is in the process of implementing its three recommendations, which have not been completed due to staffing issues. Finally, the Department of Public Works has implemented two of its five recommendations. Despite the efforts made by the Technology Services and Public Works Traffic Engineering departments, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

For your reference, this report includes a Highlights page that provides background and summary information on the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to all of you and to Technology Services, Public Works, General Services, and Parks and Recreation personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5000 or Shannon Kuhn, Internal Audit Supervisor, at 720-913-5159.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

REPORT HIGHLIGHTS

Industrial Control Systems
February 2017

Status

Of the thirteen recommendations made in the May 2015 audit report, the Technology Services department is still in the process of implementing its recommendations, Public Works Traffic Engineering has implemented two of its five recommendations, General Services has implemented all of its recommendations, and Parks and Recreation has implemented both of its recommendations.

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, manage irrigation systems and swimming pools.

Purpose

The purpose of this audit was to assess the City's internal control environment as it relates to Industrial Control Systems 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 from Original Audit

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 about 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.

Findings at Follow-up

Technology Services is in the process of implementing all three recommendations with a final completion anticipated for September 30, 2017. Public Works has implemented password settings for the traffic system to align with the City's Acceptable Use Policy and is performing physical access reviews. They are in the process of developing and implementing a formal backup and contingency plan as well as a formal change management process. General Services has removed unauthorized accounts for building automation systems, implemented logical access reviews, and secured backup files. Parks and Recreation has improved their backup and storage process, and implemented logical access reviews for building automation systems at recreation centers and irrigation systems for parks and golf courses.

For a complete copy of this report, visit www.denvergov.org/auditor, or contact the Auditor's Office at 720.913.5000.

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
FINDING: The City Does Not Have a Governance Strategy To Manage Industrial Control Systems and Has Not Assessed Them for Security and Operational Integrity			
Technology Services Recommendations			
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.	Due to staffing changes and vacancies, Technology Services (TS) has not implemented the audit recommendations. TS will work on all three of these recommendations throughout 2017 with final completion by September 30, 2017.	**Not Implemented**
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.	Due to staffing changes and vacancies, Technology Services (TS) has not implemented the audit recommendations. TS will work on all three of these recommendations throughout 2017 with final completion by September 30, 2017.	**Not Implemented**
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.	Due to staffing changes and vacancies, Technology Services (TS) has not implemented the audit recommendations. TS will work on all three of these recommendations throughout 2017 with final completion by September 30, 2017.	**Not Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
Public Works – Traffic Engineering Recommendations			
1.4	The Traffic Management System Administrator should implement password security settings as established by the City's Acceptable Use policy.	The Traffic Management System Administrator updated the password and account settings in the Traffic System domain to align with the standards provided in the City's Acceptable Use Policy.	**Implemented**
1.5	Traffic Engineering Management should perform quarterly physical access reviews of the Traffic Management Center and inner server room.	Traffic Engineering Management is performing quarterly physical access reviews of the Traffic Management Center and inner server room. In addition, they have strengthened the badge access request process by centralizing the approval process.	**Implemented**
1.6	Traffic Engineering Management should develop, document, and implement formal backup and contingency plans for the traffic signal system.	In response to the original audit report, Public Works agreed to develop and implement formal backup and contingency plans for the traffic signal system by the end of 2015. Due to the funding requirements, the project was delayed but is now scheduled to be completed by the end of 2017. Traffic Engineering Management has obtained space for a server room and for seven staff cubicles, and is working on building out the necessary infrastructure.	**Not Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.7	The Traffic Management System Administrator should perform periodic user access reviews of the traffic signal system and all associated systems.	Audit follow-up work revealed that the Traffic Management System Administrator has not implemented periodic user access reviews. The Administrator asserts that there is a compensating control in place, based on the fact that user access to the system is dependent upon having an account with access to the denvergov domain. However, the audit team does not consider this compensating control sufficient to mitigate the risk identified during the original audit.	**Not Implemented**
1.8	Traffic Engineering Management should monitor vendor access to ensure changes to software are formally requested, approved, and monitored.	Traffic Engineering Management has begun discussions with the Traffic Management System software vendor about change management, but a formal process has not yet been implemented.	**Not Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
General Services – Building Automation Systems Recommendations			
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.	All accounts that were identified in the initial audit as being unauthorized have been removed or disabled. Additionally, annual periodic logical access reviews are being performed for the respective Building Automation Systems (BAS), and require that individual user accounts and passwords be created in the BAS system.	**Implemented**
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.	Backups for the building automation systems that are managed by Facilities are now backed up and stored in a location away from the primary computer systems.	**Implemented**
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.	Although a formal agreement from the vendor was not obtained, backups for the building automation systems that are managed by Facilities are now being backed up and stored in a location away from the primary computer systems.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
Parks and Recreation – Building Automation Systems and Irrigation Recommendations			
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.	Backups for the irrigation system are now being managed by Technology Services through an enterprise data backup and recovery solution. Backups for the Parks and Recreation Building Automation Systems are now being managed using quarterly work orders that specify the creation of a new backup, if there have been system changes since the previous quarter. Backups are secured in an off-site location.	**Implemented**
1.13	The Director of Parks and Recreation should ensure that teams perform periodic logical access reviews for the Industrial Control Systems they manage.	The irrigation system has been upgraded since the original audit and users now authenticate using the same credentials as their individual City and County of Denver credentials. Logical access reviews for the Parks and Recreation Building Automation Systems are scheduled through the use of quarterly work orders. Additionally, the Building Automation Systems supervisor has placed greater emphasis on information technology security through the use of security awareness training, team meetings, and the incorporation of a security based performance measure.	**Implemented**

Conclusion

We found that both the General Services and Parks and Recreation departments have fully implemented all recommendations assigned to their agencies during the original audit. Accordingly, we believe these efforts have adequately mitigated the associated risks identified during the original audit. The other two departments involved in the audit—Technology Services and Public Works—have implemented some recommendations; however, six have yet to be fully implemented. Despite the steps both Technology Services and Public Works have made toward starting to implement recommendations 1.1, 1.2, 1.3, 1.6, 1.7, and 1.8, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated.

Technology Services is in the process of developing a comprehensive inventory and risk assessment of the Industrial Control Systems in use throughout the City, developing security guidelines to assist agencies with managing and administering Industrial Control Systems. Additionally, Technology Services is in the process of identifying the workstations attached to industrial control systems that should not be subject to lockout security settings. Public Works has not fully developed formal backup and contingency plans as agreed to in the original audit. Furthermore, Public Works has not created a change management process that includes ensuring changes to the traffic management system are formally requested, approved, and monitored prior to vendors implementing changes to the traffic system. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from the Technology Services, Public Works, General Services, and Parks and Recreation departments for their cooperation during our follow-up effort and their dedicated public service.