Cybersecurity Audit

May 7, 2021

Mayor

Betsy Price

Council Members

Carlos Flores, District 2
Brian Byrd, District 3††
Cary Moon, District 4†
Gyna Bivens, District 5
Jungus Jordan, District 6††
Dennis Shingleton, District 7††
Kelly Allen Gray, District 8
Ann Zadeh, District 9

† Audit Committee Chair
†† Audit Committee Member

City of Fort Worth
Department of Internal Audit

200 Texas Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor
Brian Burkland, Assistant City Auditor
Tom Wilson, IT Auditor

The Cybersecurity Audit was conducted as part of the Department of Internal Audit's Fiscal Year 2020 Annual Audit Plan.

Audit Objective

The objective of this audit was to evaluate the effectiveness and efficiency of existing controls that would help deter, prevent and/or respond to cyberattacks.

Audit Scope

Our audit included a review of the City's information technology policies, processes and mechanisms in place during FY2020.

Opportunities for Improvement

Additional security measures at the alternate data center

Remediation of identified safety issues

Appropriate data and system classification designations

Executive Summary

As a part of our FY2020 Annual Audit Plan, the Department of Internal Audit conducted a Cybersecurity Audit. Based on our interim audit results (which were communicated in an interim audit report, dated December 18, 2020) we concluded that the City's:

- network account password requirements were adequate and appropriate for ensuring effective control of and access to the City's network;
- security awareness training program was compliant with the State of Texas' security awareness training requirements; and,
- multi-factor authentication requirement provided enhanced security for users who connect remotely to the City's Virtual Private Network (VPN).

Our interim audit results also noted that Continuity of Operations (COOP) plans existed for most, but not all, departments. However, some COOP plans had inaccurate information and/or were outdated. We also reported that written regulations that addressed information technology (IT) security were not all updated, that an organizational vulnerability management plan did not exist, and that the Information Technology Solutions Department's change management entries did not contain sufficient detail to explain what software was being changed, nor which computer assets were affected by the change(s). In addition, we reported that three recommendations from the IT Asset Verification Audit, released in August 2017, had not been implemented.

Based on audit testing subsequent to our interim audit results, we concluded that:

- efforts are sufficient to aid in the prevention of data loss and the maintenance of enterprise software integrity;
- cybersecurity events are effectively communicated to the appropriate levels of management;
- access controls for the City's alternate data center could be strengthened;
- safety hazards exist within the alternate data center; and
- the IT Security Administrative Regulations and the IT Applications/Data Catalog did not contain correlating data and system classifications.

These findings are discussed in further detail within the Detailed Audit Findings section of this report.

Table of Contents

Background

Cybersecurity, as defined by the cybersecurity company Norton LifeLock, is the practice of protecting electronic systems, networks, computers, mobile devices, programs and data from malicious digital attacks. Norton LifeLock notes the following as different types of cybersecurity.

- *Network security* protects internal networks from intruders, by securing infrastructure. Examples of network security include the implementation of two-factor authentication and new, strong passwords.

- *Application security* uses software and hardware to defend against external threats that may present themselves in an application's development stage. Examples of application security include antivirus programs, firewalls and encryption.

- *Information security* protects both physical and digital data (essentially data in any form) from unauthorized access, use, change, disclosure, deletion, or other forms of malfeasance.

- *Operational security* addresses processes and decisions for handling and protecting data assets, and includes permissions users have when accessing a network.

- *Data loss prevention* consists of developing policies and processes for handling and preventing the loss of data, and developing recovery policies in the event of a cybersecurity breach. This includes setting network permissions and policies for data storage.

- *End-user education* involves teaching users to follow best practices, such as refraining from clicking on unknown links or downloading suspicious email attachments, which could allow malware or other forms of malicious software to penetrate the computer network.

Objective

The objective of this audit was to evaluate the effectiveness and efficiency of existing controls that would help deter, prevent and/or respond to cyberattacks.

Scope

The audit included a review of the City's information technology (IT) policies, processes and mechanisms in place during FY2020.

Methodology

To achieve the audit objective, the Department of Internal Audit used a detailed audit program based on the cybersecurity framework from the National Institute of Standards and Technology. We also interviewed staff from the Information Technology Solutions Department, and reviewed the City's:

- computer assets and software inventory in use by City of Fort Worth (CFW) departments;
- written, information security policies;
- Information Technology Solutions Department's risk assessment processes;
- public internet website;
- lists of security awareness training attendees, and subsequent reporting to the State of Texas;
- procedures and listings related to computer asset disposal;
- Information Technology Solutions Department's response to physical and electronic anomalous activity events; and,
- network vulnerability scan results.

We conducted this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We are independent per the generally accepted government auditing standards requirements for internal auditors. Chapter XXVIII of the Fort Worth City Charter established the CFW's Department of Internal Audit independent of management, reporting directly to the Fort Worth City Council. We utilized the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework when evaluating internal controls.

The following internal control components and corresponding principles were considered significant to the audit objective. COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Internal Control Component	Principles
Control Environment	Managerial oversight, integrity, ethics and responsibility; staff recruitment, development, retention, performance and accountability
Control Activities	Policies, procedures and systems
Risk Assessment	Clearly-defined objectives to identify risks, define risk tolerances, and implement necessary controls (e.g., written policies and procedures)
Information and Communication	Communication of necessary, quality information
Monitoring	Monitoring and evaluating the effectiveness of internal controls

FORT WORTH

Audit Results

We concluded that the Information Technology Solutions Department has implemented controls and related measures to effectively deter, prevent, and/or respond to cyberattacks, and that cybersecurity events are effectively communicated to the appropriate levels of management. We also determined that the Information Technology Solutions Department takes appropriate measures to ensure effective control of and access (including remote) to the City's network, and meets the State of Texas' requirements for security awareness training and related reporting. The Information Technology Solutions Department has also implemented controls to adequately prevent the loss of data and maintain the integrity of enterprise software.

Access control to the City's water treatment computer systems were found to be appropriate and adequate. Existing standards and measures include the use of the least-privilege access model for controlling remote access to specific personnel, the use of encrypted, multi-layer connections, and monitoring activity associated with the secure connections. Additional controls include network segmentation, firewalls and port restriction, and threat detection via continuous monitoring.

Our interim audit results noted that Continuity of Operations (COOP) plans existed for most, but not all departments, with some plans having inaccurate information and/or being outdated. However, each department now has a COOP plan on file with the City's Office of Emergency Management. We also indicated that during the interim reporting period, written regulations that address IT security were not all updated, an organizational vulnerability management plan did not exist, and the Information Technology Solutions Department's change management entries did not contain sufficient detail to explain what software was being changed, nor which computer assets were affected by the change(s). The Information Technology Solutions Department has since updated the IT security-related regulations, and is currently addressing the organizational vulnerability and change management items. Finally, we reported that three recommendations from the IT Asset Verification Audit, released in August 2017, had not been implemented. One of those three audit recommendations has since been fully implemented. The target implementation date for one of the remaining two audit recommendations was March 31, 2021, while the target implementation date for the other recommendation is September 30, 2022.

Internal Audit subsequently focused on the City's physical information security and safety policies, management of application software user accounts, network management policies, cybersecurity incident response plans, and data/system classifications. Based on audit tests completed since the interim audit report, access controls to the CFW's alternate data center (Eagle Mountain Communications Tower Building) were considered inadequate. We observed a door, leading to a restricted area, with no locks. We also identified incomplete and/or inconsistencies in the building's sign-in logs, and observed safety hazards (e.g., network cabling running along the floor, and a power strip cord draped over an equipment cabinet door). Internal Audit did not identify any issues/concerns regarding the data center located in City Hall.

Data classification categories defined in the City's IT Security Administrative Regulations do not correlate to any application/data-related information within the Information Technology Solutions Department's Application/Data catalog. Because no such correlation exists, it is unknown if applications and/or data were being accessed and exposed in an appropriate or inappropriate manner.

We also identified the following issues that were not considered material audit findings, but were worth mentioning to City management.

The Information Technology Solutions Department utilizes basic functionality and reporting relative to IT computing/network resource capacity planning (e.g., network usage and availability, database space usage

and availability, etc.). However, the department lacks sophisticated tools and techniques that would allow it to adequately plan for future resource needs based on current usage trends.

From discussions with Information Technology Solutions Department staff and a review of the City's IT network diagrams and related documentation, we concluded that Security Information and Event Management Systems (SIEMs) monitoring tools were not installed so that network traffic and performance baselines could be established. Such baselines show the typical amount of network traffic expected to be processed, and could aid in determining if the City's IT network is processing an abnormal amount of traffic beyond the established norms, potentially as the result of intrusion attacks from entities outside of the network.

The City's Ransomware Incident Response Program does not state the persons/groups responsible for the steps outlined in the document, and the Cybersecurity Incident Response Program identifies two former CFW employees as Designated Incident Responders. Also, the City's IT Security Administrative Regulations do not provide specifications for what data/information should be included in audit logs/records.

We reviewed user account records for three CFW software systems (PeopleSoft Financials, FASTER Fleet Management, and Accela for Development Services). No issues were identified with PeopleSoft Financials or FASTER user accounts. However, nine Accela software active user accounts were assigned to terminated CFW employees.

Overall Risk Evaluation

High	Medium	Low
Some access control weaknesses at the Eagle Mountain Communications Tower Building		
Eagle Mountain Communications Tower Building safety hazards		
No correlation of data classification definitions between the IT Security Administrative Regulations and the IT Solutions Department's Application/Data Catalog		

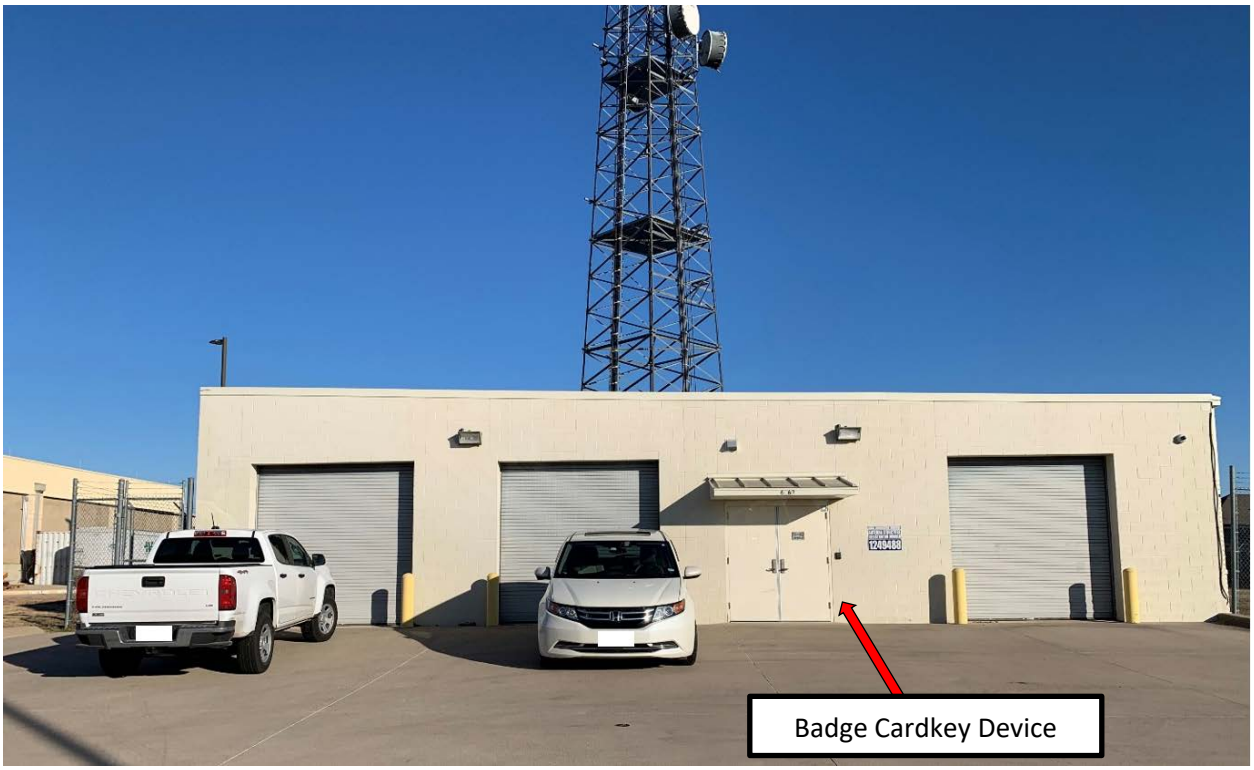
Detailed Audit Findings

1. Some access control weaknesses exist at the CFW alternate data center.

The CFW Information Technology Solutions Department operates an alternate data center within the Western Communications Tower equipment building at the Eagle Mountain Water Treatment Plant. The alternate data center is a gated and fenced-in facility located at 6801 Bowman Roberts Road in northwest Fort Worth. The tower and its equipment building were constructed in 2005-2006, to provide the CFW Police and Fire Departments with radio coverage to support public safety service for the general area in the western segment of Fort Worth to the Parker County line, as well as for the City's extraterritorial jurisdiction in northwest Tarrant County. Space for the alternate data center was initially allocated within the tower equipment building in 2009-2010, and currently serves as the backup location for the City's primary city hall data center. The alternate data center's location is shown in the following photo.

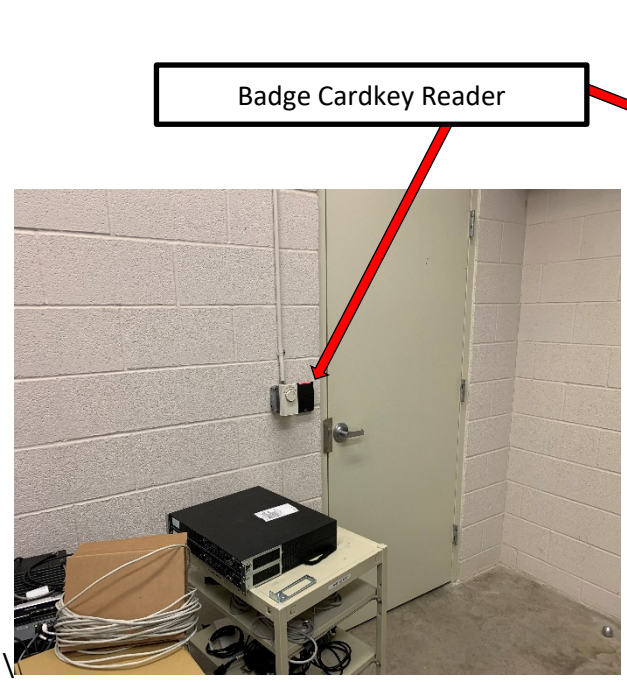
Source: Google Maps

During a December 16, 2020 visit to the alternate data center site, Internal Audit observed that the entry door to the tower building itself is controlled by a badge cardkey device.

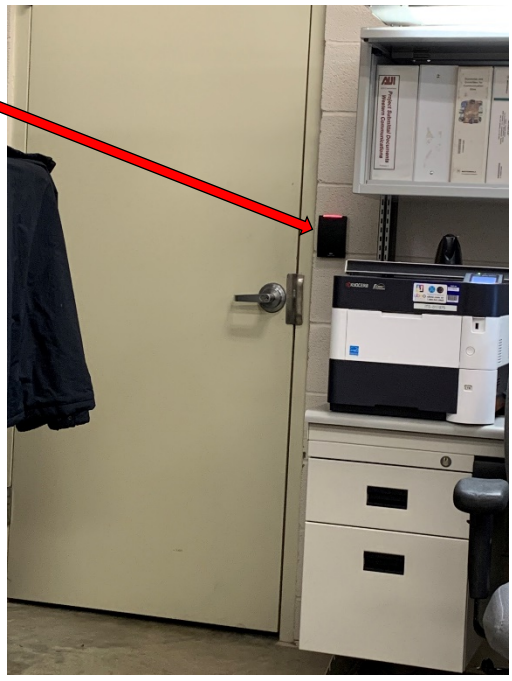


Source: Auditor Photo (Eagle Mountain Communications Tower Building – Front Entrance)

Upon entering the building, Internal Audit observed three doors -- two storage closet doors and the server room door, one on either side of the lobby area, each with an installed badge cardkey device. However, the doors to the room housing the tower communications and data center equipment, which is a restricted area, did not have locks.



Source: Auditor Photo (Storage Closet #1)

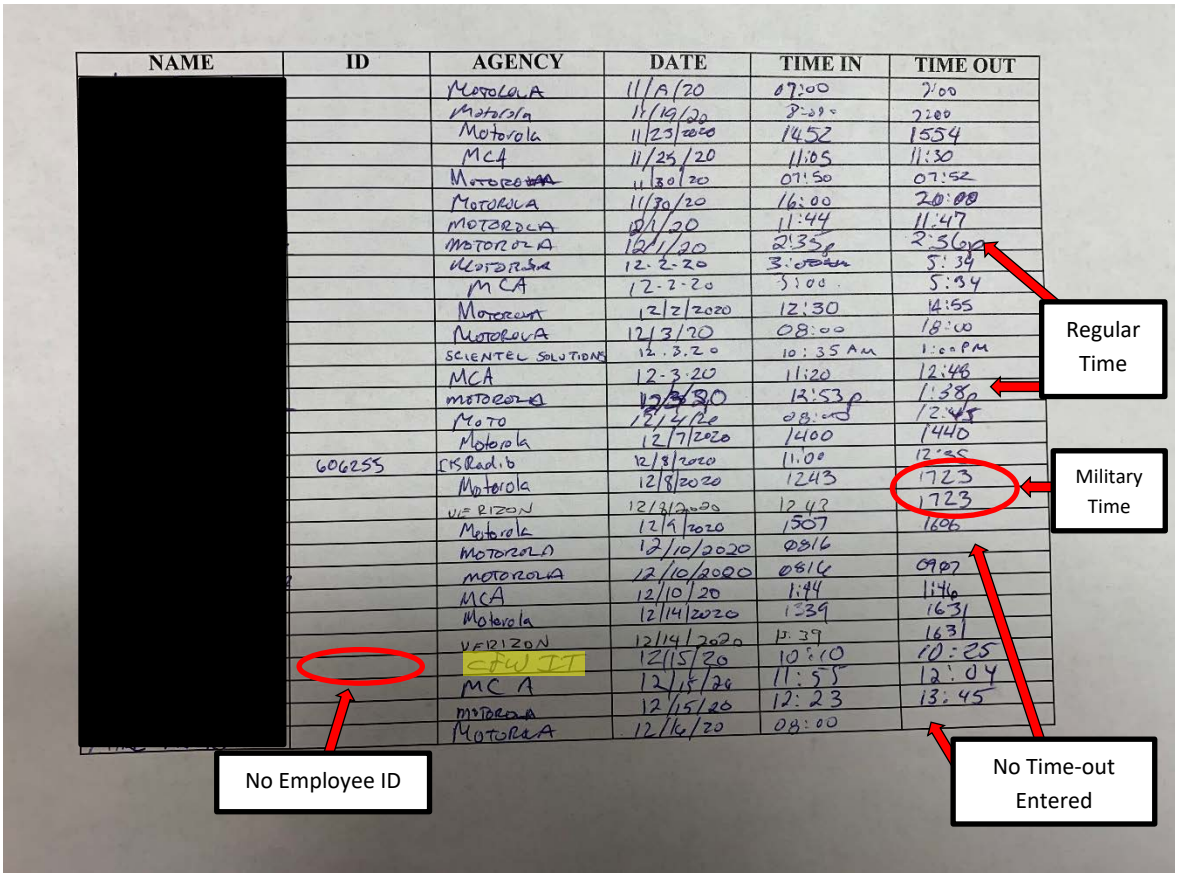


Source: Auditor Photograph (Storage Closet #2)

Source: Auditor Photo (Eagle Mountain Communications Tower Building Lobby)

Two CFW Information Technology Solutions Department employees staff the building on Wednesdays between 6:00am and 6:00pm, with each employee working a six-hour shift. Activities occurring within the building are monitored by CFW IT Solutions City Hall data center personnel, via remote cameras. Information Technology Solutions Department personnel are automatically alerted when individuals enter the Eagle Mountain Communications Tower Building. A paper sign-in log is also used to capture site visits to the building.

For the period between August 18, 2020 and December 16, 2020, we identified six instances where CFW Information Technology Solutions Department employees entered the tower building without documenting their employee ID onto the building access log. We identified seven instances where individuals accessing the building recorded the time they entered, but not the time they left. Additionally, times noted on the building access log were sometimes captured in regular and military time.



Source: CFW IT Solutions Department

A total of 174 entries were documented in the building access log between August 18, 2020 and December 16, 2020.

- The majority of the entries (128 of the 174, or 74%) occurred when the building was not staffed.

The remaining entries (46 of the 174, or 26%) took place during the day, and on Wednesdays when the building was staffed. A breakdown of the site visits is shown in the following table. All but two of the logged site visits occurred between Monday and Friday.

Eagle Mountain Communications Tower Building Site Visits (August 18, 2020 through December 16, 2020)	
Day of the Week	**Number of Site Visits**
Monday	34
Tuesday	35
Wednesday *	46
Thursday	31
Friday	26
Saturday	2
Total	**174**

Source: Sign-In Logs received from the IT Solutions Department
* Information Technology Solutions Department personnel on site – 6:00am-6:00pm

Based on our observations, we concluded that access to areas within the City's alternate data center site was not adequately controlled. The Control Objectives for Information Technologies (COBIT) 2019 standard states that access to premises, buildings, and areas should be justified, authorized, logged, and monitored, and should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors, or any other third party. CFW IT Security Administrative Regulation, AR-D5, states that contract maintenance personnel and others who do not have authorized access, but who are required to be in the restricted area, must be escorted by an authorized person at all times. While the use of monitored remote cameras and building entry alerts are compensating controls, they rely on human interaction in order to be effective, and do not fully conform to the requirements stated in AR-D5.

Recommendation 1A: *The Chief Technology Officer should ensure that the doors to the tower building's main equipment room are fully secured with a door locking mechanism, such as a badge cardkey device, and that the process for granting, management, and revocation of access to the server room is fully documented.*

Auditee's Response: Concur. ITS agrees with this recommendation and has initiated the process to have the identified door secured with a door locking mechanism managed via a standard badge cardkey device.

Responsibility: Sallie Trotter – Assistant Director, IT Solutions

Target Implementation Date: June 30, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Recommendation 1B: *The Chief Technology Officer should require that all persons entering the communication tower document their time of ingress and egress, and City identification number (if applicable) on the building access log; and should consider requiring a consistent recording of time (i.e., regular or military time).*

Auditee's Response: Partially Concur. ITS agrees with this recommendation, yet determined a different approach to mitigation. The security aspects of the manual ingress/egress log are better served by securing critical areas with automated capabilities, and thus will deprecate the manual log process once the remaining door within the facility is secured with a standard badge cardkey device. At that point all transitions within/without the building as well as the critical areas within the building are recorded on the badge access control system. The existing logs will be retained in accordance with the standard retention period and then destroyed.

Responsibility: Donlen Ruffin – Assistant Director, IT Solutions

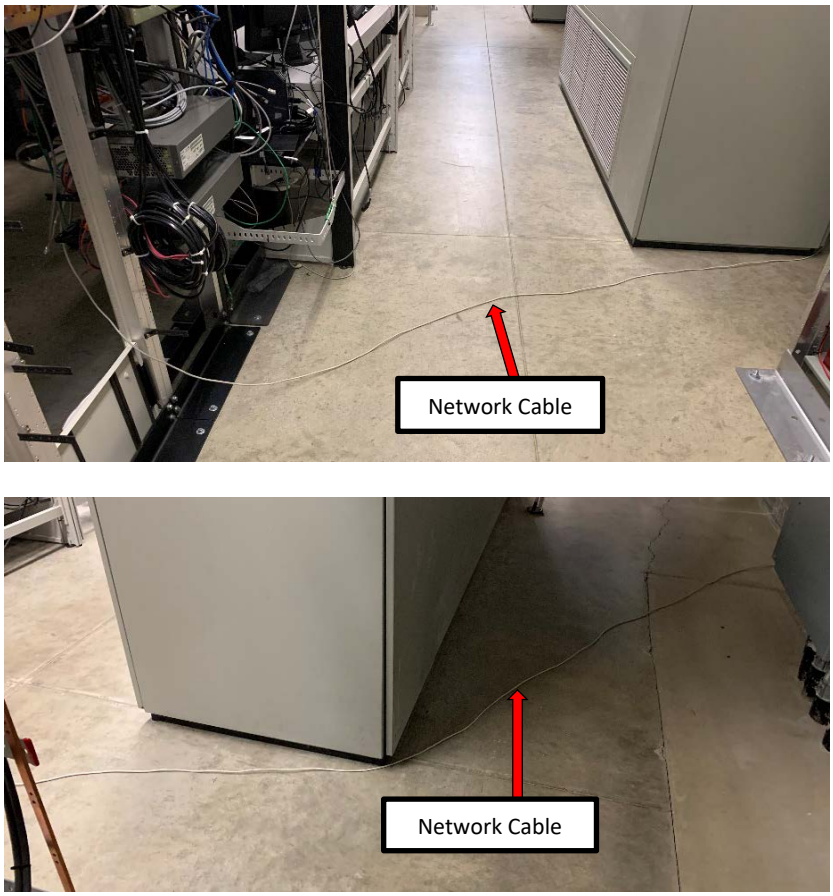
Target Implementation Date: July 30, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

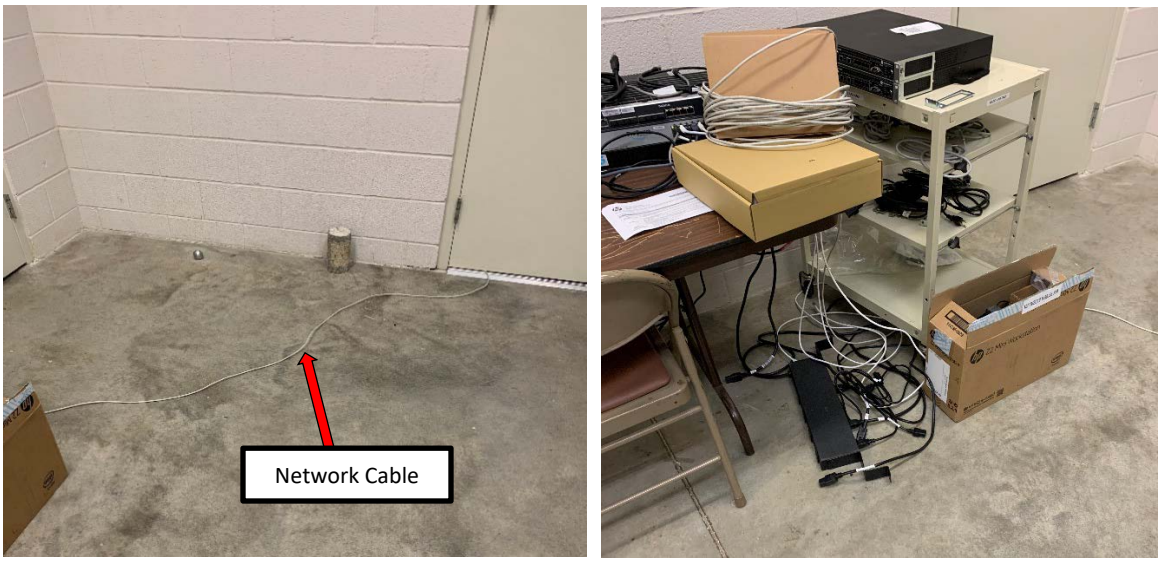
Applicable Assistant City Manager: Valerie Washington

2. Safety hazards in the Eagle Mountain Communications Tower Building were identified.

During a December 16, 2020 site visit, Internal Audit observed a network cable running across the equipment room floor. One end of the cable was connected to a piece of rack-mounted equipment. The cable was routed across the floor, running under the equipment room doors, going out into the building lobby area in front of a storage closet, with the other end of the cable laying on the floor next to a piece of network equipment.

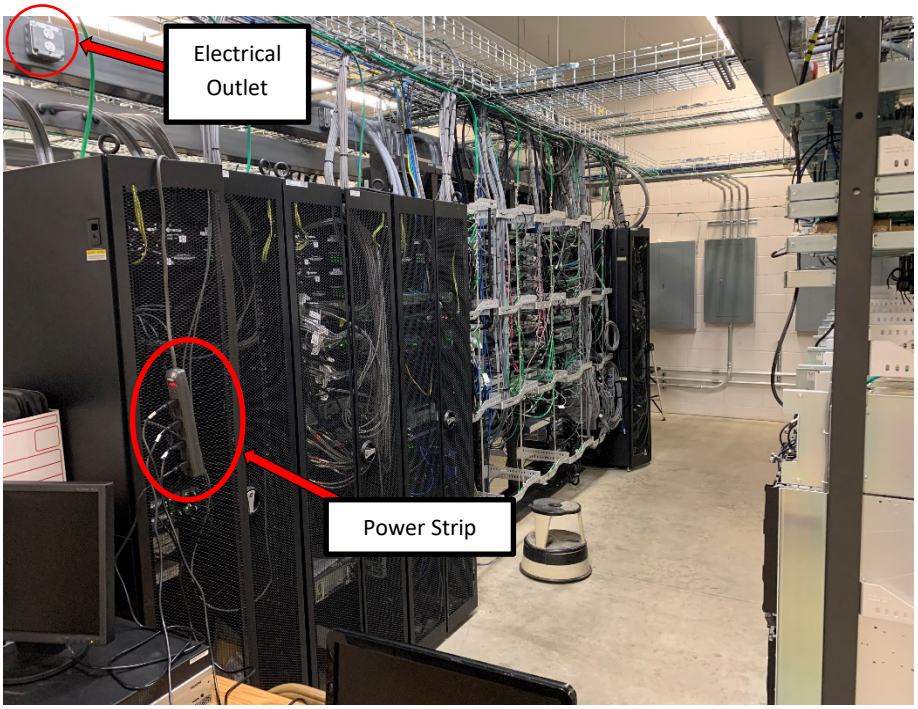


Source: Auditor Photo (Equipment Room, north side, in the Eagle Mountain Communications Tower Building)



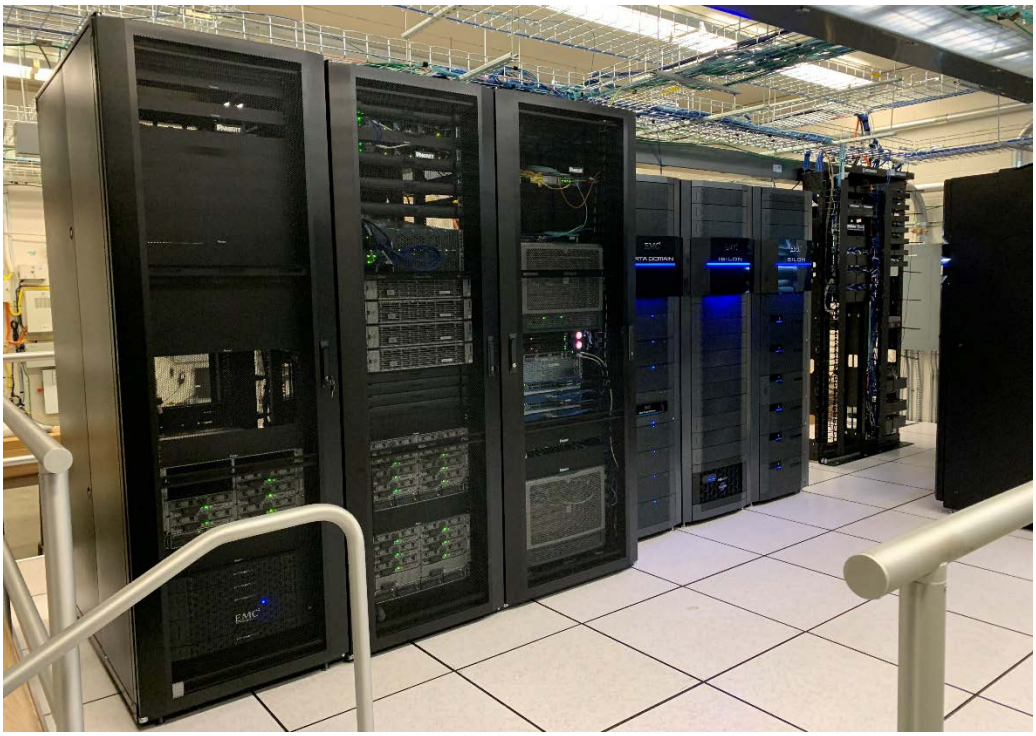
Source: Auditor Photos (Eagle Mountain Communications Tower Building Lobby)

During the same site visit, a power strip was observed to be plugged into an electrical outlet inside of an equipment cabinet, with the power strip cord hanging over the top of the cabinet door. An electrical outlet exists above the equipment cabinet, so it is not clear why that outlet was not used, instead.



Source: Auditor Photo (Eagle Mountain Communications Tower Building Equipment Room – north side)

Network cables within the building rest on, and are routed throughout the equipment room via ceiling-mounted cable trays. The trays are designed to support electrical and network cables used for power distribution, control, and communication, and serve to organize the cabling for easier identification and management.



Source: Auditor Photo (Eagle Mountain Communications Tower Building)

The COBIT 2019 standard states that facilities should be managed to be in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines, and that cabling and physical patching (data and phone) are structured and organized. The presence of any sort of cabling running across a floor in open areas represents a trip hazard that could result in injuries to persons and damage to equipment. Additionally, the manner in which the power strip is installed increases the risk that the power cord could be pinched or cut by the equipment door, thereby creating a fire hazard.

Recommendation 2: *The Chief Technology Officer should ensure that the identified cabling hazards within the Eagle Mountain Communications Tower Building are remediated, and that cabling is installed in a safe and appropriate manner.*

Auditee's Response: Concur. ITS agrees with this recommendation and has remediated the identified cabling hazards. ITS management will stress the importance of maintaining a hazard free environment with all personnel utilizing the facility, and will integrate a hazard review within the normal site inspections that occur on a monthly basis (at a minimum). This facility is shared by Platform Technologies and Radio Services (both ITS organizations), and the hazard review integration will occur within both teams.

Responsibility: Sallie Trotter & Donlen Ruffin – Assistant Directors, IT Solutions

Target Implementation Date: May 30, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

3. IT asset classification documentation and related processes are incomplete.

IT assets (data and systems) are categorized within CFW IT Security Administrative Regulation (AR-D5) as either Class A or Class B. Class A IT assets are sub-categorized as either Critical or Restricted, while Class B IT assets are sub-categorized as either Controlled or Limited/Controlled. However, our review of the AR-D5 documentation and the CFW FY2020 Records Retention Schedule found no correlation between the definitions of Class A or Class B assets and the systems/data sources recorded in the CFW IT Solutions Department's Application/Data catalog.

For example, AR-D5 states that all security logs generated by IT assets must be retained for 60 days for those assets categorized as Class A. However, none of the applications listed in the Application/Data catalog contain any information regarding Class A or B designations. So, it is unknown which applications would generate Class A security logs.

In addition, Section 6.1.7 of AR-D5 Appendix 3, Mobile Computing and Removable Storage Media Policy, states that CFW Class A data must not be downloaded to removable storage media devices without written exception granted from the information owners, Department Director, and the CFW IT Security Manager, or in the absence of the Manager, executive management of IT Solutions or its authorized agent. Without knowing what data falls into the Class A category, adequate enforcement of the policy would be difficult to achieve.

The COBIT 2019 standard states that information assets accessible by the business should be secured through approved methods, including information in electronic form, information in physical form, and information during transit. This benefits the business by providing end-to-end safeguarding of information. Additionally, data classification and acceptable use security policies should be applied to protect information assets under control of the business.

Recommendation 3: *The Chief Technology Officer should ensure that the IT Solutions Department's Application/Data Catalog is updated to reflect the appropriate system/data classification, as defined in IT Security Administrative Regulation AR-D5, for each system and data source listed in the catalog.*

Auditee's Response: Concur. ITS agrees with this recommendation and will review/update AR-D5 to better align the organizational capabilities and strategic intent as it relates to the topic of system/data classification.

Responsibility: Donlen Ruffin – Assistant Director, IT Solutions

Target Implementation Date: July 30, 2021 (for approval submission)

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Acknowledgements

The Department of Internal Audit would like to thank the Information Technology Solutions and Water Departments for their cooperation and assistance during this audit.