City of Austin
Office of the City Auditor

Investigative Report

Communication and Technology Management Department Unnecessarily Incurred Costs to the City of Austin

January 2020

The Communication and Technology Management department (CTM) paid roughly $95,000 in rent for space in a data center they did not occupy for eight months. CTM leadership ignored concerns that criminal justice information might be moved to a space not suitable to host it and this inaction led to the wasted rent. The department was scheduled to occupy the data center in August of 2018, but the initial move was delayed as CTM ultimately had to address the security concerns that had been previously raised, but not acted on. Staff members began raising these concerns prior to the contract being signed with the vendor in December 2017. They continued raising these concerns for approximately 8 months until the initial move was delayed. CTM did not move into the new facility until June 2019.

Contents

Cover: Aerial view of downtown Austin, iStock.com/RoschetzkyIstockPhoto

Allegation

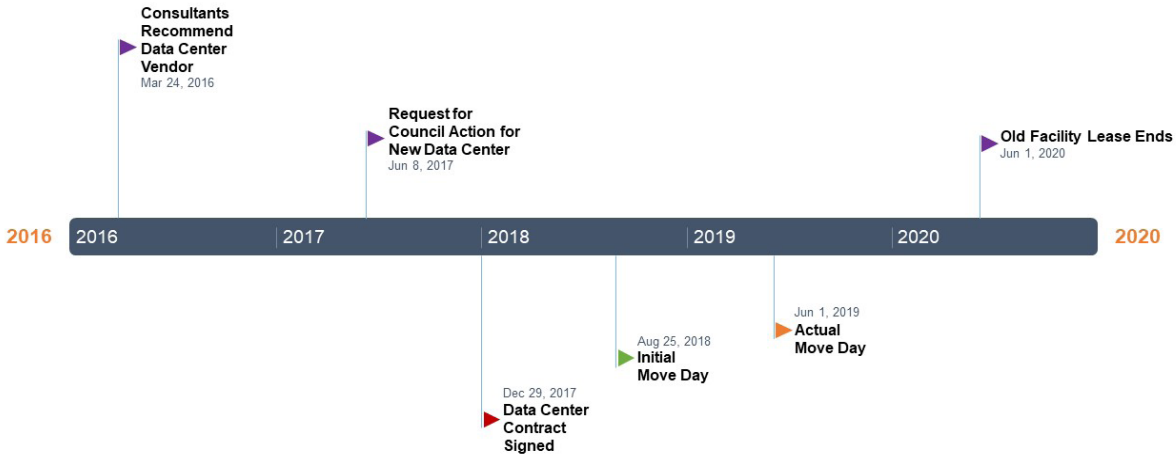
An anonymous informant reported that the Communication and Technology Management department (CTM) was wasting tax dollars by paying for a facility that was not being used. According to the informant, CTM signed a contract to rent space in a new data center that would house the City's data and servers. CTM was scheduled to move into the new data center in August 2018, but the move was placed on hold due to security concerns raised by the security team at CTM. The informant also alleged that the security concerns that led to the delayed move were brought up multiple times in the past and were disregarded by CTM's data center relocation team.

Background

CTM is responsible for the City's network and telecommunications services. The facility housing the City's servers and data in 2017 was no longer meeting the City's needs, and its lease was coming to an end in June 2020. As a result, CTM entered into a five-year lease agreement in December 2017 with a vendor to provide data center space for the City's servers and data. CTM was scheduled to move into the new data center in August 2018.

CTM, as a service provider for the City's public safety departments and other City departments that access criminal justice data, is required to follow specific security rules on how it protects that data. The Austin Police Department (APD) shares criminal justice data with multiple other City departments and has written agreements with these City departments detailing their security responsibilities for storing or accessing the data.

Exhibit 1: Background of Data Center Relocation



SOURCE: Based on emails, real estate documents, and testimony. Chart created 7/3/2019.

Investigation Summary

The Communication and Technology Management department (CTM) paid roughly $95,000 in rent for space in a data center they did not occupy for eight months. CTM leadership ignored concerns that criminal justice data might be moved to a space not suitable to host it, and this inaction led to the wasted rent. The department was scheduled to occupy the data center in August 2018, but the initial move was delayed as CTM ultimately had to address the security concerns that had been previously raised, but not acted on. Staff members began raising these concerns prior to the contract being signed with the vendor in December 2017. They continued raising these concerns for approximately 8 months until the initial move was delayed. CTM did not move into the new facility until June 2019.

Finding

Waste of City Resources

Incurring Costs to the City of Austin

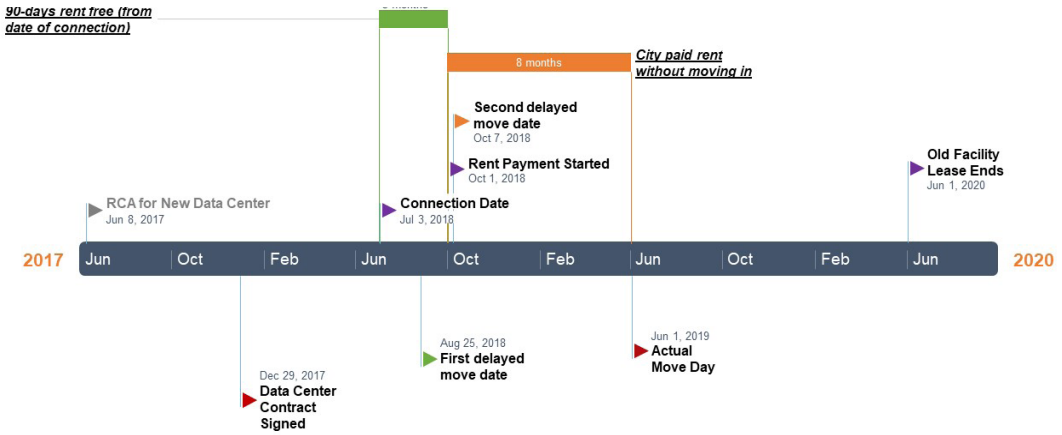
In 2016, a consultant hired by CTM found that the facility housing the City's servers and data no longer met the needs of the City and recommended that the City move its servers and data to another facility. CTM formed a Data Center Relocation (DCR) team that was tasked with moving the City's data and servers to the new facility. CTM hired consultants to identify a new space that met all the City's needs. On December 29, 2017, CTM signed a contract with the selected vendor. The contract was in the form of a lease agreement, and was for 63 months, beginning with a 90-day rent-free grace period. Thereafter, the City would pay a monthly charge of at least $10,150. There would also be a one-time build-out cost of roughly $61,500. CTM set a move date for the last weekend in August 2018.

Months of Delays and Incurred Costs

Staff from the Office of Chief Information Security Officer (OCISO) in CTM raised concerns that potential criminal justice data was about to be moved into the new facility, and that the facility did not meet the required level of security for that type of data. From the testimony and evidence we collected, we found that CTM increased efforts to address the concerns raised by the security team only after the move was delayed, months after the same security concerns were initially raised by other CTM employees. The move date was rescheduled for October 7, 2018.

CTM did not meet the October 2018 target date to complete the move. According to staff, CTM had only moved in hardware, such as cabinets and network equipment, and established a second internet connection in the facility. The data center was not being used for its primary purpose, which was to host the City's data and servers. When interviewed, employees admitted that very little of the space the City was renting was being used at the time. A few employees estimated the usage as low as 10%. After the 90-day grace period, the City started paying rent on the property, as agreed, but had still not moved in its data and servers. Ultimately, the City moved into the space on the weekend of June 1, 2019. By this point, the City had been paying rent for eight months. The rent payment had also gone up to $15,350 per month starting in April 2019. Due to the delay and increased rent, the City incurred a cost of roughly $95,000 in rental payments before moving in its data and servers.

Exhibit 2: Timeline of Data Center Relocation



SOURCE: Based on emails, Real Estate Documents, and testimony. Chart created 7/3/ 2019

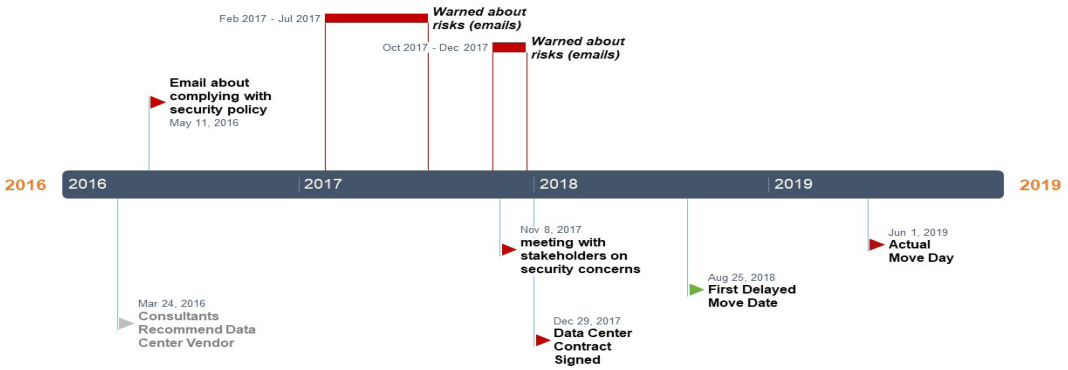
Inadequate Oversight and Inefficient Practices by Management

For the purpose of this report, the staff from the Office of Chief Information Security Officer (OCISO), will be referred to as the security team.

The DCR team was involved in drafting the contract with the vendor, ensuring the City's interests were met, and eventually moving the City's data and servers into the new space. We found evidence that this team was warned numerous times, starting as early as December 2017 and throughout the relocation process, about risks and security concerns related to the data CTM intended to transfer to the new facility.

We found several emails from CTM staff indicating that security risks were raised in DCR team meetings prior to the contract being signed with the vendor. There was at least one email from that time period from the security liaison for APD suggesting that specific security measures needed to be incorporated into the new contract with the vendor. The security liaison for APD is responsible for interpreting federal policies on the use and protection of criminal justice data. The security liaison also provided suggestions on how to successfully move into the new data center without violating security rules and regulations. Additionally, the security liaison for APD raised concerns about the chosen vendor's unwillingness to take steps to ensure its staff went through the required background checks or agree to additional security steps to allow them to house criminal justice data.

Exhibit 3: Warning about Security Policy



SOURCE: Based on emails, Real Estate Documents, and testimony. Chart created 7/3/2019.

From testimony and evidence gathered, we found that APD initially considered housing their data with other City data at the new data center. However, prior to the contract being signed with the vendor, APD withdrew its involvement because of similar security concerns as those identified by CTM staff regarding the storage of criminal justice data.

CTM Director's Response

When we spoke to the Director of CTM, he stated the first time he was made aware of any concerns regarding the risks of criminal justice data being moved into the new data center was just before the initial move date in August 2018. He added that it was brought to his attention by the security team and he delayed the move in response. However, we found evidence that various employees, including members of the security team, reached out to him multiple times via email about concerns that the new data center could not hold sensitive security data given its current security standards. These emails date back to late 2017. In at least one email, he told the employee that he would look into the concern. After reviewing a sample of the emails, the Director stated that while he did not specifically recall each communication, he felt any issues brought up would have been addressed at project briefing discussions.

At his interview, the Director of CTM concluded that when preparing to move the City's data to the new data center, CTM was obligated to vet and remedy any security risk that the security liaison to APD might identify as related to security policy violations.

Inaccurate Risk Assumption about Criminal Justice Data

We also found evidence that key members of the DCR team did not take steps to mitigate the risks of relocating sensitive security data to the new data center in response to warnings from other CTM employees. These risks were communicated before the contract was signed and before the initial move date was delayed. Key members of the DCR team made mistaken assumptions about the risks associated with the City's criminal justice data and did not take steps to validate their assumptions or CTM staff's concerns. Two members of the DCR team noted that they did not feel the communicated risks were specific enough for them to act upon.

Specifically, the DCR team believed that all public safety data, including criminal justice data, were housed in APD's own data center and that no criminal justice data would be held by other departments in the City's data center. However, shortly after the contract was signed, a public safety IT project manager provided the Deputy Chief Information Officer (DCIO) with a list of applications used by APD that were housed in the City's data center. This list identified whether each application was known to contain criminal justice data, whether each application was intended to contain this data, and whether there were any known compliance issues. This list was created in 2015, and the IT Project Manager who sent it noted the list of sensitive data locations, "has not been updated in quite some time." Seven months prior to the original move date, the DCIO passed this list to the project manager and division manager over the DCR team saying, "Now that we know of it, we are obliged to check it out…"

Additionally, we learned that APD had a list of City departments that included Municipal Court and Law, with which they had written agreements allowing access to criminal justice data. However, this list was not provided to CTM staff until after the initial move had been cancelled. The DCR team's assumption did not seriously consider that other non-public safety departments could access APD's criminal justice data and potentially store that data outside of APD's control. When interviewed, multiple DCR team members said that those departments should not have stored criminal justice data on a non-APD server, so they did not check for criminal justice data. They stated that they had not verified whether those departments were complying with this policy.

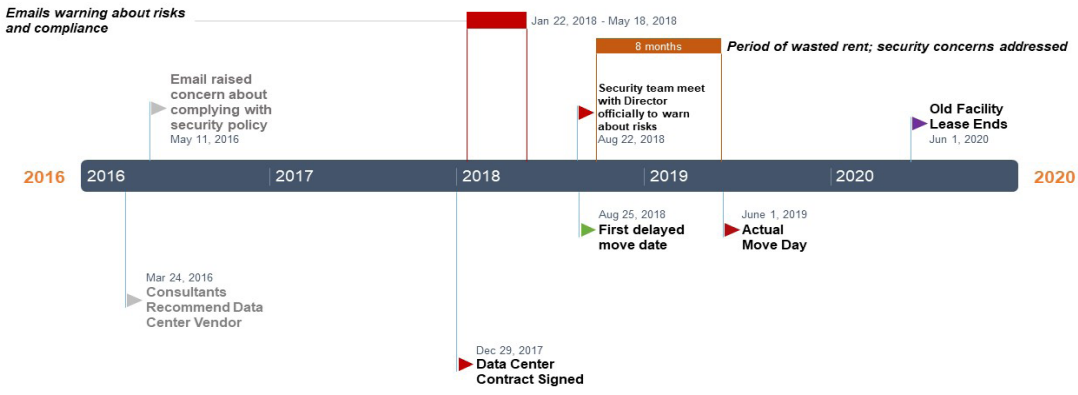
Risk Remediation Steps by CTM

We found that the security team and other CTM employees identified options to reduce the risk of criminal justice data being moved unintentionally or improperly to the new data center. These options included encryption; a complete inventory of CTM's assets (application and virtual servers) which did not exist at the time; and an assessment of that inventory and the file shares to identify any instances of criminal justice data being stored by non-APD departments. Based on multiple witness accounts, none of these steps were taken prior to the first move date. At least one employee initiated a database of the CTM's asset inventory but noted that they received little support for the project; and CTM management decided to go ahead with the initial move without waiting for the inventory to be completed.

When key members of the DCR team were asked why the identified risk remediation steps did not take place prior to the initial move date in August 2018, cost was mentioned repeatedly as an important factor. Specifically, the team said that encryption was too expensive, and a review of the City's file shares and inventory for security policy violations would have been too time-consuming. The most frequently stated reason for not pursuing any remediation, however, was that the team assumed the risks did not exist.

The assumption that there would be no criminal justice data on non-APD servers proved inaccurate. Two employees informed us that at least one example of criminal justice data had been found on the computer of an

Exhibit 4: Warning about Risks and Wasted Rent



SOURCE: Based on emails, Real Estate Documents, and testimony. Chart created 7/3/2019.

employee in a non-public safety department. Had this data been moved to the new data center, it would have violated federal policies.

Contradictory Opinions on Security Standards

We also found that there were contradictory points of view within CTM on what assets needed to follow security regulations and what could safely be moved to the new data center. Additionally, there were contradictory opinions on whether the chosen vendor had met the proper security standards to hold the City's data, and whether it could hold data from non-public safety departments that access criminal justice information as part of their operations.

CTM's failure to address security concerns in a timely manner, which led to the City paying for unoccupied data center space for eight months, appears to constitute waste, as detailed in the following criteria:

- City Code 2-3-5(A)(3)(a) & (b): Waste of City Resources

Appendix A - Management Response

CTM Data Center Audit

Management Response

September 23, 2019

The data center move strategy is a complex story, and a number of important facts and figures need to be added to assure a complete understanding.

Reports that CTM (Communications and Technology Management Department) has wasted City funds at the colo are mistaken. Although the CIO (Chief Information Officer) took problematic advice from staff in delaying the data center move, CTM has in fact saved money by using the colo, in spite of delaying the full move into the colo.

By timely contracting the colo, CTM gained savings of $600,000 over five years on the colo cost itself. Additionally, CTM gained a savings of $500,000 over five years for Internet connectivity.

Waller Creek Center Not Intended for Criminal Justice Information

First, CTM operates two major primary data centers. The WCC (Waller Creek Center) data center hosts a broad variety of critical City data; however, criminal justice information was never intended to be hosted there.[1] The other data center, at CTECC (Combined Transportation, Emergency Communications Center—the 911 center), was built expressly for public safety information, including the City's criminal justice information (CJI). Given that WCC is not intended for CJI, occasional discoveries of CJI data within WCC have been mitigated whenever they were discovered. This practice is ongoing. However, the limiting factor is that it is reactive, since active discovery is unavailable.

Further, in APD's (Austin Police Department) Management Control Agreement (MCA) with CTM, CTM is charged with technical controls. In their memoranda of understanding with four other departments that access CJI, APD tasks those departments with maintaining compliance. Those departments have not requested CTM to assist them with hosting CJI, but if they had, they would have been connected with CTECC as the appropriate custodian.

The CTECC facility fully meets the requirements of the MCA for hosting CJI, and the WCC data center was never intended to be nor sold as a CJIS (Criminal Justice Information Systems)-compliant data center. In designing the replacement data center at the collocation data center, CTM has taken steps that raise the level of security there over that of WCC, but not so that it could serve as a CJI repository. One of the above-and-beyond security controls that CTM has installed in the Cyrus One data center is

[1] This was affirmed by the then-LASO (local agency security officer) in two emails in December, 2017. On December 5, 2017 she sent an email that stated "Since no CJI or CJI-containing networks will be routed to the colocation space, the CJIS policy will not apply. " On December 11, 2017 she sent an email to multiple people stating that "There's no sign-off needed…since there will be no CJI stored, processed, or transmitted to or from that location."

Appendix A - Management Response

CTM-controlled badge access to the computer racks. In short, the Cyrus One data center is more secure than WCC.

Waller Creek Center At Risk For Failure; Creates Urgency

The Chief Information Officer for the City of Austin supports technology operations for most of City government. CTM performs a large part of those technology operations in the Waller Creek Center data center, and if that data center were to fail, 75-90% of City government would be seriously impaired during a lengthy recovery. Payroll, financial management, human resources tracking, building permitting, park operations, library operations, and many, many other routine City services to residents would be grossly impacted. The potential for negative financial impact within City government would be large, and the impact could also be felt in the City economy beyond City government.

Starting in 2013, CTM began investigating the risk associated with continued use of the aging WCC data center and engaged a reputable expert organization to study the question. Dell was engaged, and in 2013 they reported that the data center had another five years of reliable life left.

After the Dell report highlighted the risk of the WCC data center, CTM contracted another expert, Hewlett Packard Enterprise (HPE) to make recommendations on a relocation strategy. Having reviewed City requirements and the data center market, HPE recommended the Cyrus One collocation data center as the best fit for the City.

Several events highlight the rising risk at the WCC data center. In 2017, the City faced a potential entire weekend of data center shutdown when the uninterruptible power supply at WCC failed in an internal bypass condition. The shutdown was only averted when Building Services conducted a dangerous and risky "hot" bypass of the UPS (uninterruptible power supply) so that a new UPS could be installed. On several occasions, failures in the chiller plumbing caused CTM staff to deploy temporary cooling equipment. As recently as August, 2018, the aging backup electric generator at WCC failed during a test due to worn out bearings.

Given WCC's history of facility failures in the last few years, high priority has been given to the data center relocation project. By getting the data center into a reliable and resilient environment, the astronomical loss of productivity associated with a citywide information technology failure would change from a high risk to a very low risk.

The threats to the viability of the aging WCC data center were becoming reality, and the CIO was and is obligated to act on them.

CTM Negotiated Aggressively; Made a Good Contract For The City

In late 2017 and early 2018, CTM (along with Office of Real Estate Services) was engaged in aggressively negotiating the contract with the colo provider that HPE recommended. Per the expert consultants that had been engaged, CTM dealt with the best fit colo provider in the Austin area, as recommended in the HPE assessment. Gaining additional expert advice from Gartner Inc., CTM negotiated a monthly rate that was 50% lower than a neighboring jurisdiction's negotiated rate, which will result in a $600,000

savings over the course of five years. The negotiations were difficult, and at the rate the data center was filling, there was risk that the offer would be withdrawn if the City did not act quickly. The City signed the deal in January, 2018, with a deferred active date.

CTM Had No Actionable Reports of Unauthorized Data Nor Role To Seek It

As planning for an August 2018 move date progressed, the security team raised concerns that there might be criminal justice information in the WCC data center and that the move should therefore be postponed. But the assertion was too vague to be actionable, for the following reasons. First, the data center operates approximately 320 business applications, each with a clear purpose (none of which was related to CJI). Second, and more important, the data center houses approximately 80 million "unstructured" files for City departments, most typically word processing files, spreadsheets, and images. Reviewing these files for suspected criminal justice information (CJI) by hand was infeasible, and CTM did not own any of the costly software products that attempts to identify CJI (though with a significant false positive rate).

CTM was aware that APD had written agreements with four departments, whereby APD entrusted those departments to safeguard criminal justice information, and those departments had agreed in writing not to mishandle such data. APD also retained a right to audit the departments' use of CJI, a responsibility that had not been given to CTM. Further, given the infeasibility of monitoring the millions of files that City departments use, CTM had no feasible way to act on APD's behalf to do so, nor had APD asked CTM to do so.

CIO Acted Appropriately and Responsibly on the Delay

In August 2018, as the planned move date approached, the CIO acted upon the CISO's (Chief Information Security Officer) recommendation to delay the move, pending further review. The CISO's team began reviewing the applications to determine if any housed criminal justice information. None was found.

The more difficult job was unaddressed because of a lack of means to review the approximately 80 million unstructured files. In December 2018, a vendor whose products were already in use at CTM provided CTM a one-time proof of concept of a software tool that would search unstructured files for potential criminal justice information. Among the 80 million files, only five files were found to contain criminal justice information, and those five files were removed. These were .000006% of the total files in the data center.

City Gained Net Positive Value from the Colo While Awaiting Full Move

In the meantime, CTM staff continued to firm up the technology as it would be moved in the collocation data center. CTM promptly built out the core network and proved out data center interconnect capability after the postponed move date; the City presence in the colo was strong. CTM also added a second Internet connection at the colo at a price far better than others that the City had had available,

Appendix A - Management Response

costing $50,000 per year less, yet receiving double data capacity than previously. By this measure, CTM has already begun realizing savings which will come to around $500,000 over the first five years from its use of the colo.

Move Delayed Further by External Factors

On October 1, 2018, longtime LASO (Local Agency Security Officer) "stepped away" from the role.[2] The role was temporarily filled by Brandon Gilstrap, an APD Records Manager, until January 19, 2019. During this three and a half months, there was no work on validation of suspected CJI held in the collocation data center.

During this same period of time, APD was preparing for its triennial CJIS audit to be conducted with DPS onsite at APD facilities in February and March, 2019. Preparation for the audit drew away APD and various CTM technical resources who could contribute to data center relocation process. Most notably, this included the CTM network team who was installing network data encryption equipment in advance of the audit. These staff would have been useful for further preparation of the data center's network.

Additionally, to actively continue with the relocation process during the onsite audit phase was deemed a possible source of confusion for the DPS auditors, and the stakes were too high to take that risk.

New, Experienced APD Local Agency Security Officer Approves the Move

Over the time covered in this period, CTM has had to rely on the advice of two successive local agency security officers to represent the CJIS requirements. At first, the LASO was a CTM employee, but in January 2019, APD hired a new LASO. This later LASO—Chip Burleson—has deep experience at the Texas Department of Public Safety in performing CJIS audits throughout Texas. Mr. Burleson has dismissed several of the concerns expressed by the earlier LASO. After examining the Cyrus One colo data center, Mr. Burleson deemed it as a more secure data center than WCC, and clearly asserted that it would be preferable to have any errant CJI in the Cyrus One colo than at WCC.

Following the delay of the move, the CIO and his team took multiple actions to prepare for the relocation, to realize value from the colo, and to find answers to assertions that hypothetical CJI was housed at WCC and was in danger of being moved to an allegedly less secure facility.

Meanwhile, APD was scheduled for a triennial audit from the Texas Department of Public Safety (DPS), to be held in February, 2019. Key resources needed for security decisions were fully focused on the audit, so Security attention to issues related to the data center was not available, adding to the delayed decision to move forward with the relocation.

LASO Burleson, in a relocation planning meeting on May 9, 2019, asserted that the collocation data center was actually more secure than the WCC data center, and that the move was *better* for APD data.

[2] Email from Mallory Bowes-Brown, October 1, 2018.

Appendix A - Management Response

The Relocation was Completed Successfully

In late March, 2019, CTM learned from the LASO the status of the DPS CJIS audit. Mr. Burleson stated that technology issues had been found compliant. He reported that he "spoke with DPS at length in regards to CyrusOne and O365 migration and they are fine with the direction we are moving." He asked for Cyrus One to sign a security addendum, and that was completed in April.

Mr. Burleson gave verbal approvals for the move to progress in April and affirmed them in a large go/no-go meeting on May 11, 2019.

Following these accomplishments, CTM restarted the move process. The move plan was the same as the original plan from 2018; no remediations had been found necessary. CTM next had to determine a workable schedule and reengage vendors involved in the move. The date was set for the first weekend of June, 2019. The physical move was completed June 2.

In June, 2019, CTM fully occupied the colo cage as the first phase of the multi-phase move project. Work is ongoing to complete the additional steps that will have WCC vacated by end of June, 2020.

Appendix B - Office of City Auditor's Response to Management Response

We have received CTM's response. We appreciate all the additional information CTM provided and reviewed it in detail. We believe our findings stand. CTM's response does not address the waste CTM created when their delays led to 8 months of rent payments for a data center location they were not using.

City resources totaling approximately $95,000 in rent were wasted, because CTM management decided to look for improperly stored CJIS data after the lease began and rent started accruing, rather than before the lease began when the same CJIS concerns were known. The lower lease price negotiated by CTM and focused on in their response simply means the waste accrued at a slower rate and does not negate the waste. Similarly, the negotiated rate for the second internet connection discussed in CTM's response is unrelated to the delayed move and wasted funds. Additionally, the departed CTM staff member and the APD CJIS audit cited by CTM as contributors to the 8 months delay only impacted the CJIS search because CTM chose to search for CJIS so late in the process.

Investigation Criteria

Finding

City Code §2-3-5(A)(3) WASTE means:

(a) the grossly inefficient or uneconomical use of a City asset or resource; or

(b) the unnecessary incurring of costs to the City as a result of a grossly inefficient practice, system, or control.

Methodology

To accomplish our investigative objectives, we performed the following steps:

- reviewed applicable City Code;
- interviewed CTM and APD staff;
- analyzed lease agreements and financial documents related to the data center;
- reviewed emails discussing security risks and the data center contract; and
- reviewed other additional documents and files related to the data center relocation project.

CAIU Investigative Standards

Investigations by the Office of the City Auditor are considered non-audit projects under the Government Auditing Standards and are conducted in accordance with the ethics and general standards (Chapters 1-3), procedures recommended by the Association of Certified Fraud Examiners (ACFE), and the ACFE Fraud Examiner's Manual. Investigations conducted also adhere to quality standards for investigations established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and City Code.

The Office of the City Auditor, per City Code, may conduct investigations into fraud, abuse, or illegality that may be occurring. If the City Auditor, through the Integrity Unit, finds that there is sufficient evidence to indicate that a material violation of a matter within the office's jurisdiction may have occurred, the City Auditor will issue an investigative report and provide a copy to the appropriate authority.

In order to ensure our report is fair, complete, and objective, we requested a response from the Department Director on the results of this investigation. Please find attached this response in Appendix A.

The Office of the City Auditor was created by the Austin City Charter as an independent office reporting to City Council to help establish accountability and improve city services. We conduct investigations of allegations of fraud, waste, or abuse by City employees or contractors.

City Auditor
Corrie Stokes

Deputy City Auditor
Jason Hadavi

Chief of Investigations
Brian Molloy

Office of the City Auditor
phone: (512) 974-2805
email: AustinAuditor@austintexas.gov
website: http://www.austintexas.gov/auditor

 AustinAuditor
 @AustinAuditor

Copies of our investigative reports are available at
http://www.austintexas.gov/page/investigative-reports

Alternate formats available upon request