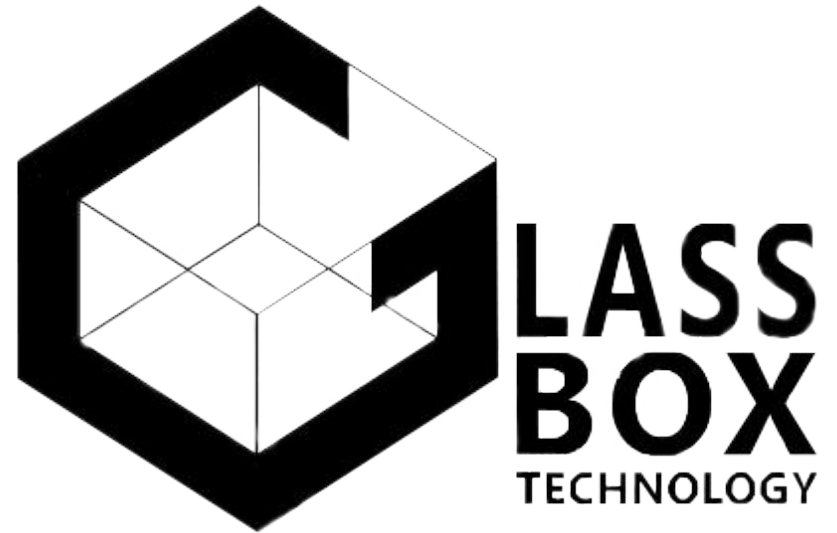




September 26, 2019

Executive Overview of Findings

The City of Fullerton's IT resources and infrastructure do not support minimum requirements and objectives. Current IT is deployed in a way that is untenable, unstable and will not support future needs. IT challenges will continue to compound and get worse until a strategic approach is undertaken

The IT assessment revealed major issues with:

- Security
- Data Center, System, and Network Stability/Redundancy
- Compliance with Regulation
- Operational Management and IT Strategy
- Questionable Financial Spending

A summary of findings as well as recommended next steps are included in this presentation.

IT Metrics

- IT Personnel: 11
- Servers: 149 (virtual and physical)
- Data Storage: 137Tb
- Network Firewalls, Switches, Routers: 91
- PCs and laptops: 700
- Printers and scanners: 300

Security Findings

Security Findings

- In a time where cybersecurity, cyber threats, and cyber terrorism are constantly in the news, the City IT Department has no dedicated cyber security staff and no one is looking at cyber security alerts
 - System security logs are recorded but aren't reviewed for intrusions
 - The right tools for review are not present and logs are not kept long enough for forensic analysis
 - There are no Incident Response procedures



Security Findings

- Security patches are not applied consistently and frequently enough across all platforms – networks, servers, storage, PCs
 - When patches are applied, there is no tool to validate that the patch worked as intended
 - Only one person is responsible for patching at the City and he is recommending that due to the volume of security patches and systems, that the city patch less frequently (Glass Box disagrees with this recommendation)
- Most of the city's network, server, storage, and PC equipment is "out of support" from the vendor by 12/31/19
 - This means that security patches are no longer applied and if the hardware breaks, there are no replacement parts
 - 78% of the City's PCs no longer receive security patches
 - 83% of the City's servers no longer have hardware support
 - 66% of the City's network equipment no longer has hardware support
 - Both of the City's storage systems (SAN) are out of hardware support



Security Findings

- Penetration tests were last run 2 years ago and the findings were issues that have been known in the industry for 10+ years
 - Most organizations run penetration tests at least twice per year
 - Most organizations have the capability to run on demand tests and run a proactive scanning solution each month
- Firewalls are not centrally and consistently managed
 - Best practices for firewall rules are not followed
- Access control systems aren't in place for critical infrastructure areas, such as the data center
 - This is also a Compliance issue
- There is no single sign on system, which exacerbates password security issues and the timely deprovisioning of access
- The tape backup system is out of support, it has not been tested to know if the file or database backups are actually working
 - There are no documented procedures for backups



Security Findings

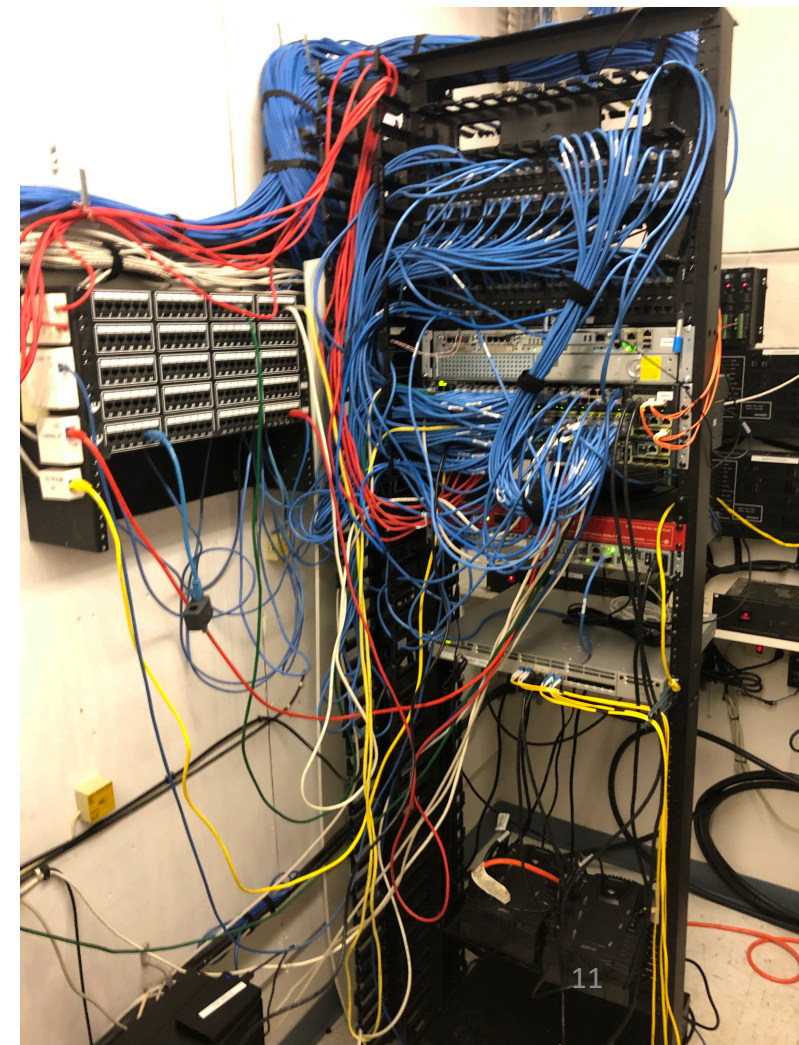
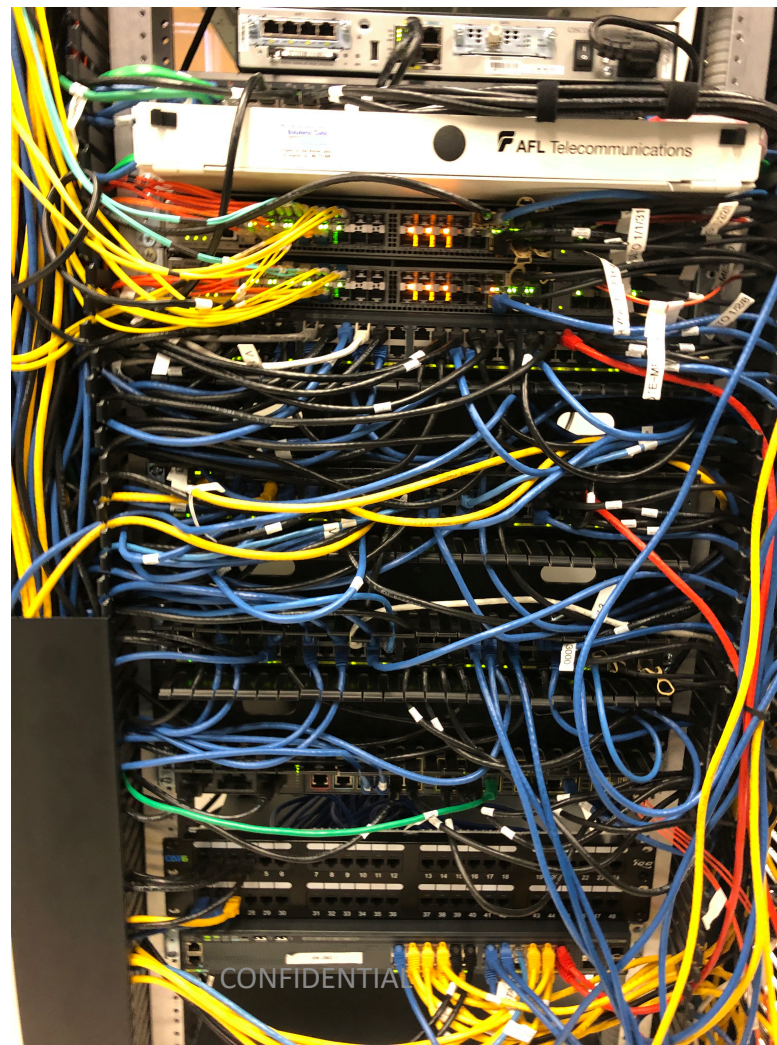
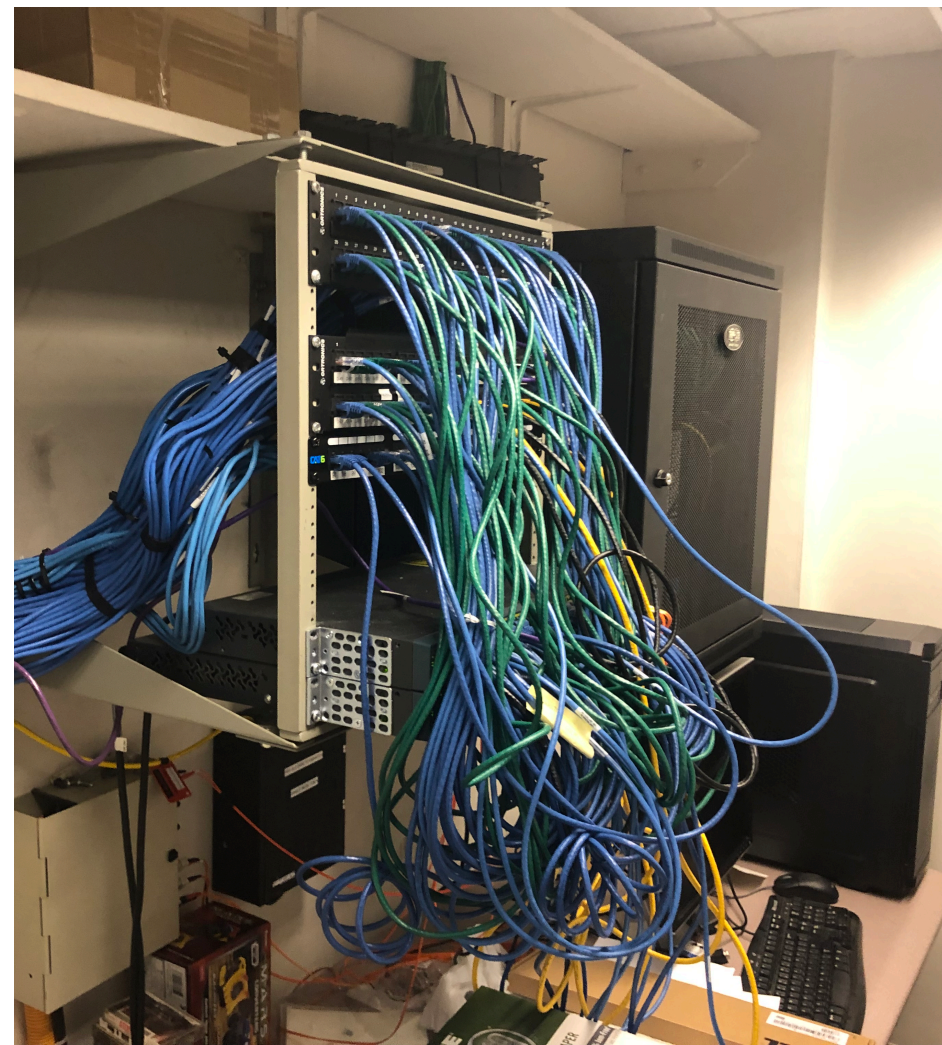
- WiFi at City Hall and at PD is not secure
 - WiFi access to City Hall network uses a shared password instead of individual user account, which means that if anyone knows the password, they can connect to the City's wireless whether they are currently an employee/contractor or not
- Hard drives are not encrypted
- All members of IT have Full Admin privileges regardless of roles and responsibilities
 - IT staff don't use a separate account for Administrative actions, which means if their City of Fullerton email is phished, it exposes full administrative access to the City from bad actors
- System access and permissions on file servers and other systems is not documented and poorly understood
- No Data Loss Prevention system in place to monitor or stop sensitive data from being sent outside of the City's network
- Process to Provision and De-Provision system access needs improvement and should be documented
- An attempt was made to set up a SSO product but they set it up to pass passwords in clear text

Data Center, System, and Network Stability/Redundancy

Network Stability/ Redundancy

- 66% of network equipment is not covered by support
 - No parts available if there is a failure
 - No security patches available
- Network connections between sites are not redundant
- The Internet connection is not redundant
- If FD1 has a network failure, none of the fire departments can connect to the data center or Internet
- Network equipment does not have redundant power supplies
- Network equipment and configurations are not standardized
- Network equipment is poorly managed (see following slide) and the network engineer doesn't understand all of its design
 - There have been multiple outages where the engineer says he hasn't had time to investigate the root cause and correct it

Current State – Network Management



System Stability/Redundancy

- Both storage systems are out of support
- Servers do not have redundant power or network connections
- 83% of the City's servers no longer have hardware support
- The City's virtual server software platform is out of support from VMWare on 3/12/20
 - This platform runs 70 servers for the City
- The City's virtual server hardware platform (3 servers) is overloaded and if one server failed, the other two could not support the full production load of all 70 servers
- The City's databases are running software that is out of support on 1/14/20
- Email system was out of support in 2018
- There are no "Dev" or "Test" environment to build or test changes
 - Changes are built and tested in live production systems with no formalized procedures for evaluating risk or communicating to stakeholders

Data Center Stability/Redundancy

- Power and cooling systems need upgrade
- Seismic bracing not installed on some racks
- There is a switch in the data center that shuts off the power to the whole data center
 - Someone inadvertently shut off this switch and caused a City-wide IT outage
- Halon fire suppression is in use in the main data center
 - Halon was banned as a fire suppression system 25 years ago
 - A replacement is needed
- No one in IT can articulate when power and cooling systems are tested and maintained
 - Power outages have affected the data center and there is a poor understanding of how power is supplied to the data center
 - Multiple buildings have mini-data centers (IDF) and those environmental conditions are worse – no seismic, fire suppression, or back up power



Compliance with Regulation

Compliance with Regulation

- The IT department does not understand what is required to meet CJIS requirements
 - Although only a separate virtual network is needed for the Police Department voice network, the IT department purchased completely separate hardware for this network – likely a \$100K deployment cost
- The Data Center does not have badge access readers for entry and PD equipment does not have access controls or even a door on the rack to stop unauthorized access to servers (see image)
 - Individuals from Administrative Services have access to the Data Center because their check printer is located there



Compliance with Regulation

- The City has multiple credit card terminals on the network but no policies or documentation to demonstrate compliance with PCI standards
- There is no process or documentation of certified disk destruction of old PC hard drives

Operational Management and IT Strategy

Operational Management and IT Strategy

No IT Strategic Plan exists

- A strategic plan guides IT spending and priorities
- In the absence of a plan, IT tends to think that 'everything is important' instead of focusing on what really matters to the City

Operational management models exist to help IT deliver consistent service levels, security, and financial value to their organizations

- The IT Department at the City does not use any operational management models and, as a result, outcomes to projects, support issues, and security management is unpredictable
- Project priority is set by the IT Manager and Project Manager instead of the organization

Operational models that would benefit City IT Operations are on the following pages

Operational Management and IT Strategy

NIST-CSF (Cyber Security Framework)

A framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk.

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection and Procedures
		PR.MA	Maintenance
DE	Detect	PR.PT	Protective Technology
		DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
RS	Respond	DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
RC	Recover	RS.IM	Improvements
		RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Operational Management and IT Strategy

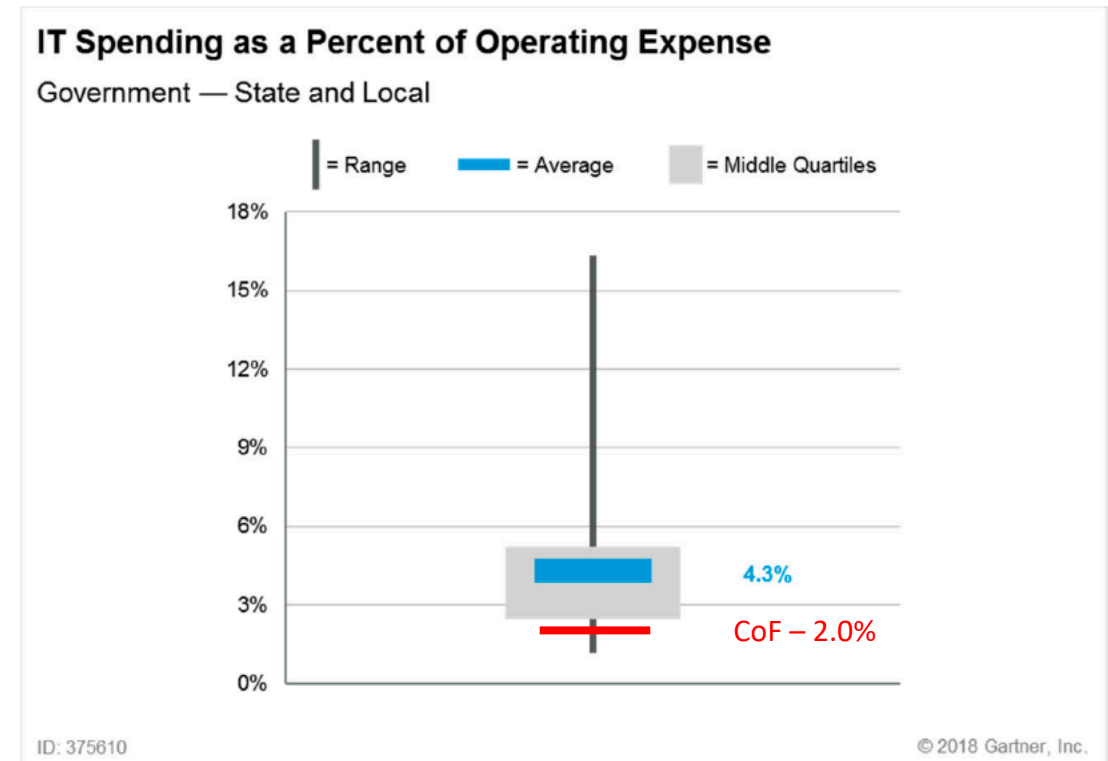
- ITIL – Service Delivery
 - Standard practices and processes to deliver high quality IT services consistently
- Project Management
 - A formalized project management methodology should be implemented to provide visibility to schedule, cost, dependencies, and risk
- Zero-Trust Computing Model
 - IT security traditionally uses a castle-and-moat concept – people inside the castle are safe and people outside are not
 - The Zero-Trust Computing Model is a holistic approach to IT security that incorporates several different principles and technologies
 - First proposed in 2010, Google, Amazon, and many others across industries have adopted the model
 - The model eliminates the idea of a safe area “inside the firewall”
 - It assumes that everything and everyone must be verified

Questionable Financial Spending

Questionable Financial Spending

- According to a 2019 Gartner report, the average IT spending as a percent of operating expense, in State and Local government is 4.3%
 - The City's spending as a percent of operating expense in 2018 was 2.0%
- Despite the lower than average funding, there were still several areas where funds were wasted

Figure 2. Government — State and Local: IT Spending as a Percent of Operating Expense



Source: Gartner IT Key Metrics Data (December 2018)

Table 3. Government — State and Local: IT Spending as a Percent of Operating Expense: by Operating Budget Scale

<\$250M in Operating Budget	\$250M-\$500M in Operating Budget	\$500M-\$1B in Operating Budget	\$1B-\$10B in Operating Budget	\$10B+ in Operating Budget
6.1%	4.7%	4.2%	3.4%	NA

CONFIDENTIAL

Source: Gartner IT Key Metrics Data (December 2018)

Questionable Financial Spending

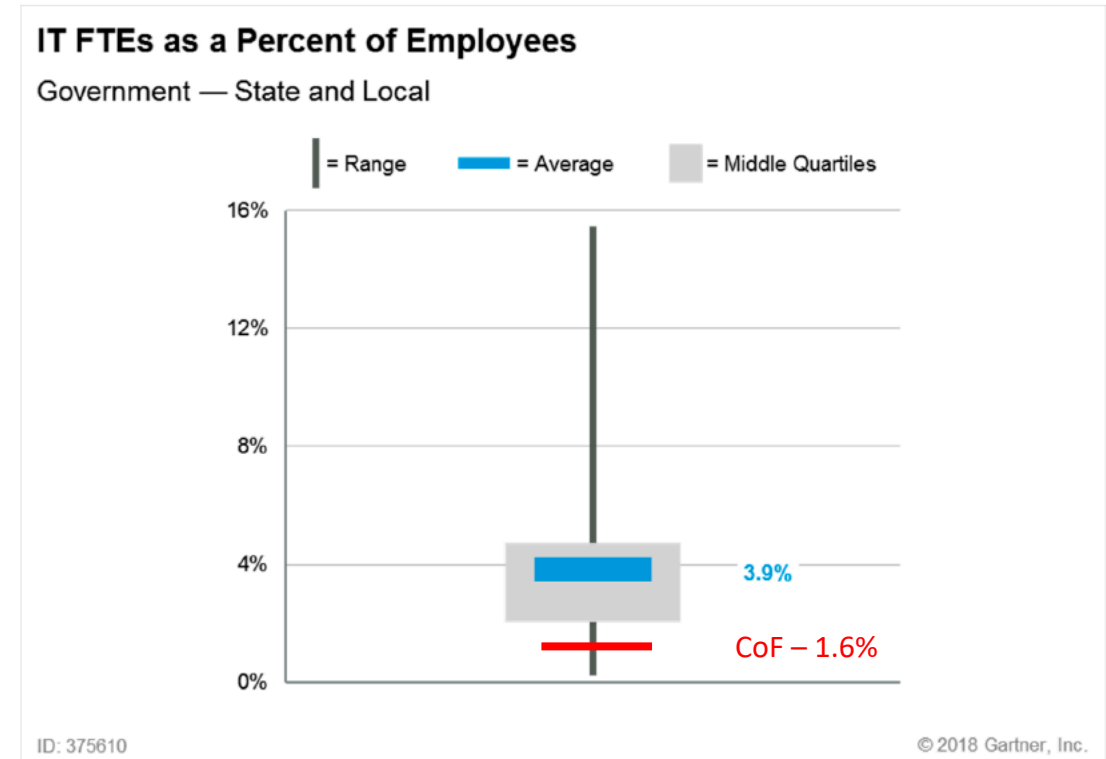
- Fiber Optic Infrastructure – despite owning up to 48 pair of fiber in some locations, only one pair is connected in the building
 - The costliest portion of fiber deployment is digging. Once inside the building, to splice a connector to a fiber is only a few hundred dollars
- Multiple network connections exist in some locations but are unused
- CJIS requires a separate virtual network for the Police Voice Network, however a complete physical network was implemented, costing approximately \$100K
- The City IT could use the built in (free) Windows antivirus, but instead utilizes a separate antivirus that costs the city \$14K/yr.
- There are 5 contractors roles that have existed for 10+ year but these have not been converted to full time
 - The contracted rate for a Desktop technician is \$130K/yr. whereas hiring an individual in house is approximately \$55-70K/year + benefits
- Chosen Disaster Recovery location is in the same disaster zone as the main data center and likely to be impacted by the same disaster that could affect City Hall

Personnel Review

Personnel Review

- IT staffing levels at the City are lower than peers in the same industry
 - IT FTEs as a percent of employees at the City is 1.6%
- An assessment of salaries has revealed that, despite much talk about lower pay, the pay is consistent with the role (title)
 - However, the City employs mostly junior or mid level roles
- The City has utilized 5 contract positions for years and would save considerable funds by converting contract positions to full time

Figure 4. Government — State and Local: IT FTEs as a Percent of Employees



Source: Gartner IT Key Metrics Data (December 2018)

Table 5. Government — State and Local: IT FTEs as a Percent of Employees: by Operating Budget Scale

<\$250M in Operating Budget	\$250M-\$500M in Operating Budget	\$500M-\$1B in Operating Budget	\$1B-\$10B in Operating Budget	\$10B+ in Operating Budget
5.4%	3.3%	3.3%	3.3%	NA

CONFIDENTIAL

Source: Gartner IT Key Metrics Data (December 2018)

Personnel Review

- It is clear from this assessment that the Manager of the department lacks the IT expertise to effectively navigate today's technology solutions and manage an IT department, as evidenced by
 - Questionable financial spending
 - Shortsighted technology solutions
 - Lack of focus on security and compliance
 - Inability to communicate the need for proper solutions to meet the City's need
 - Staff are left to decide on their own what is best
- The findings highlighted in this assessment were done during her tenure

Personnel Review

- The Network Specialist has mid-level expertise in networking and only basic knowledge in server administration
 - He has significant gaps in knowledge and how he manages the environment
 - Recommends that security patching happens less often
 - Has multiple technologies that are out of support by end of 2019, but doesn't have a plan to have them replaced or upgraded
 - Shows gaps in understanding the proper way to implement and/or manage cybersecurity
 - Would need significant technical leadership to be successful at his job

Recommendations

Security & Compliance Recommendations

Using the NIST-CSF framework and Zero Trust Model, implement the following security improvements:

1. Contract with an outside firm for cybersecurity monitoring, incident detection, and incident response (Security Operations Center)
2. Asset Management
3. Vulnerability Management
4. Patch Management
5. Implement Full Disk Encryption on all laptops and desktops across the City
6. Implement Office 365 Data Loss Prevention
7. Implement FedRAMP compliant Single Sign On
8. Implement anti-ransomware software
9. Implement PCI and CJIS required network segmentation
10. Assess and improve policies on mobile device management

Security & Compliance Recommendations

Using the NIST-CSF framework and Zero Trust Model, implement the following security improvements:

11. Implement badge access controls to the Data Center
12. Remove administrative access from IT personnel who don't require it for their job role
13. Implement separate administrative accounts for IT personnel who require administrative access
14. Implement a Security Training system for employees to educate on topics such as phishing, passwords, and general cybersecurity issues
15. Implement PCI policies and train IT staff on requirements
16. Perform a CJIS Compliance assessment
17. Review what additional CJIS training exists for IT staff
18. Implement a Compliance Portal that tracks the weekly management actions required for compliance to PCI, CJIS, and other regulatory requirements

Data Center, Network, and Server Stability

1. Move all servers and data storage to a FISMA and FedRAMP compliant colocation facility
 - a. NOTE: The existing data center needs significant upgrades to power, cooling, structured cabling, and fire suppression. It will remain the “hub” of your network connectivity to the Internet, PD, Fire Departments, Library, and other city facilities.
2. Replace out of support network equipment – including wireless networks
3. Implement redundant connections from City facilities to the data center at City Hall and new colocation facility
4. Replace out of support firewalls
5. Replace out of support servers and data storage
6. Replace the tape/data backup system
7. Migrate to Office 365 to replace the out of support email platform and have better email security tools

Data Center, Network, and Server Stability

8. Migrate out of support databases to a supported platform
9. Remediate IDF cabling issues
10. Undertake longer term planning to get the City's fiber delivered to each of the City's buildings

End User Computing

1. Replace 550 out of support PCs
2. Build a PC management infrastructure to support automating operating system, application, and patch deployments
3. Build Encryption infrastructure for centralized deployment and management support
4. Create a new, secure PC “image”
 - a. Full disk encryption
 - b. Secured operating system
 - c. Integrated (and free) antivirus
5. Purchase extended support for PCs that will not be replaced by end of 2019
 - a. This requires an Enterprise License Agreement with Microsoft

Financial Stewardship

1. Establish formalized Project Management procedures and reporting to obtain better value from City projects
2. Implement the ITIL framework, processes, and software to improve service availability, predictability, and transparency
3. Negotiate enterprise license agreements with Microsoft and VMWare to better leverage their software capabilities and to establish the security platforms mentioned the security recommendations slides
4. Negotiate bulk discounts with Cisco and Dell (or other PC provider) on the upcoming rounds of purchases
5. Document what is required for Business Continuity and use it to drive what the City's Disaster Recovery solution should be
6. Identify telecom/network connections no longer in use and terminate those agreements

Personnel Recommendations

- More staff is needed to reduce single points of failure
 - The network administrator is the most vulnerable position due to volume of duties, experience, and skillset
- Hire the 5 contract positions to permanent and invest those savings into new positions
- A more technical and experienced IT manager is needed to give direction to the staff
 - Given the diversity and complexity of the environment, a Director position is likely more suitable
- More experience and skill is needed at all of the roles employed
 - Sr. Network Engineer, Sr. Desktop Engineer, Sr. Programmers, Sr. Project Manager

Next Steps

- Glass Box can develop and deliver a strategic plan for implementing these recommendations
 - A high level project plan
 - A detailed financial plan including estimated cash flow by month and fiscal year
 - Recommendations for people and process improvements
- Utilize the Glass Box vCTO service to accelerate technology decisions, begin architecture and design planning, and start negotiating key enterprise agreements while awaiting final approval on go forward strategy

Strategic Plan

Funding Update

- Both Dell Financial Services and Cisco Capital have offered capital leasing options that include a mix of their products as well as other products and professional services
 - Dell Financial Services has offered \$7.5MM
 - Cisco Capital has offered \$5.0MM
- Cisco is also gathering information on initiatives that may offer funding to the City
 - Smart City projects are offering funding which could offset some of the spend

Overview of Costs

Excluded Items

- New phones (desk or cell)
- Facility Costs to remediate power, cooling, or fire suppression in the existing data center
- Costs to expand existing City Fiber Optic network
- Business Continuity or Disaster Recovery Planning/Assessments

Included Items

- Hardware, software, tax, and shipping for all products
- Professional Services
- Security Camera Upgrade (\$900,000)

Cost Overview – by Category

Category	CAPEX	OPEX
Security & Compliance	\$2,831,000	\$497,500
Networking	\$2,518,000	\$222,265
Servers & Storage	\$2,578,000	\$415,551
End User Computing & Office 365	\$2,020,000	\$ 97,750
New Organization		\$437,408
GRAND TOTAL	\$9,947,000	\$1,670,474

Project Timeline

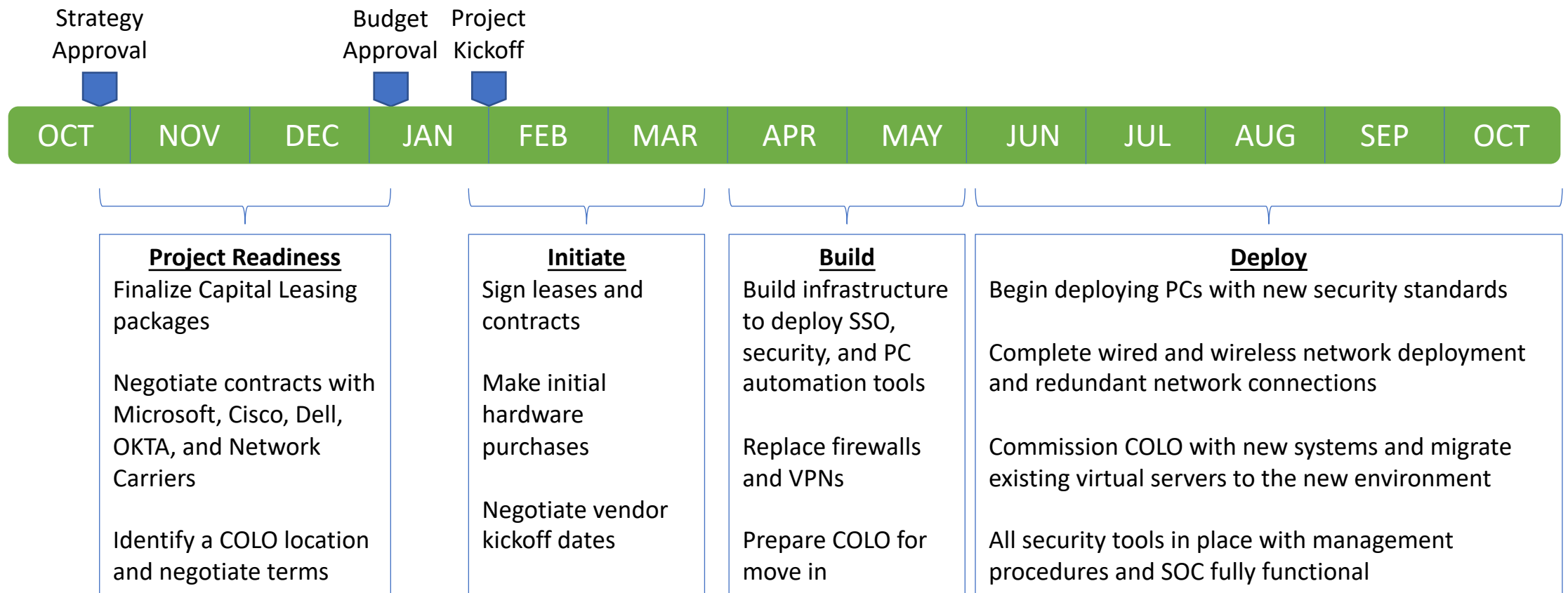
- See Project Plan

Project Cash Flow - Capital

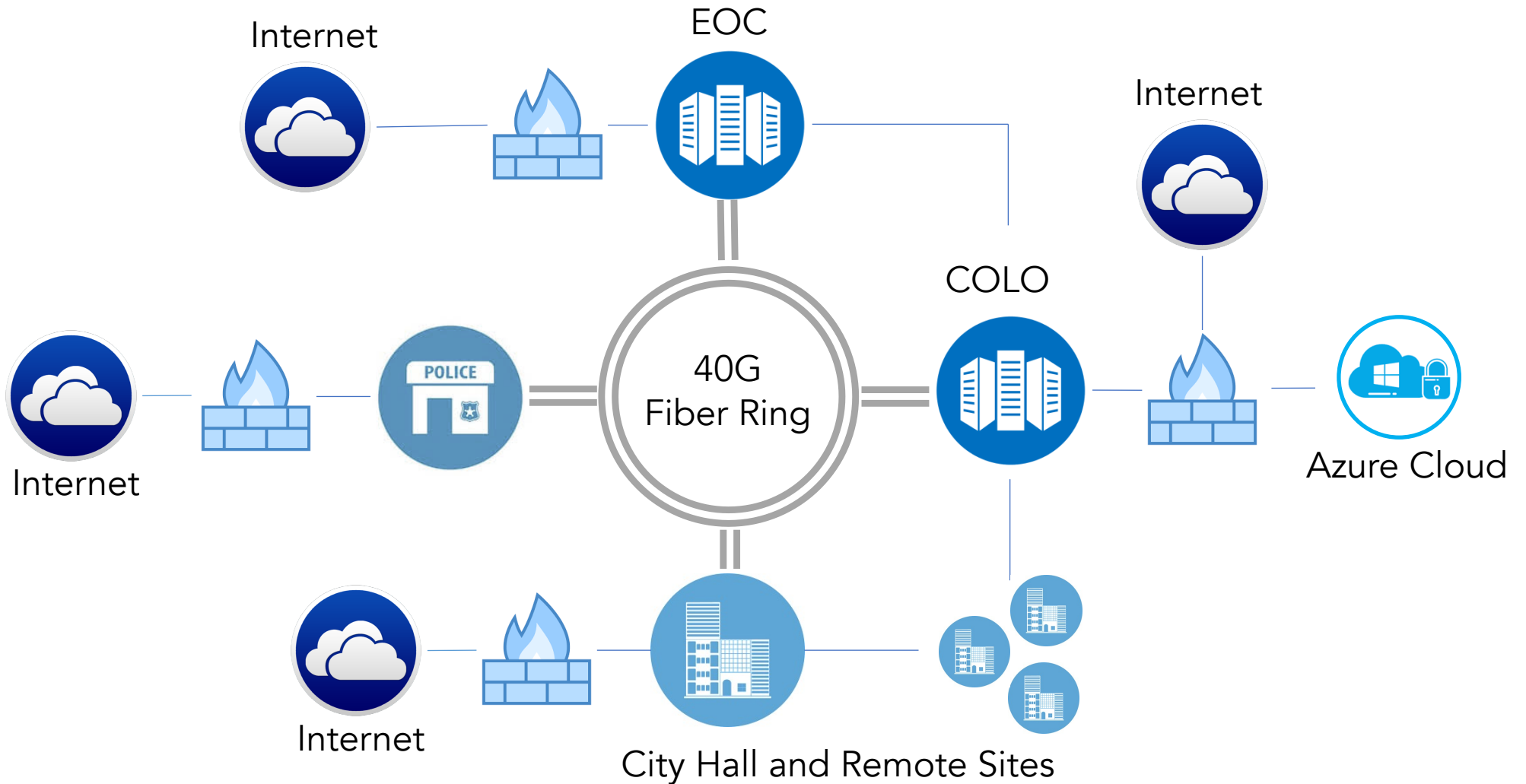
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13
\$0	\$985	\$1,226	\$2,319	\$1,299	\$672	\$697	\$617	\$617	\$617	\$411	\$243	\$243

All figures in thousands

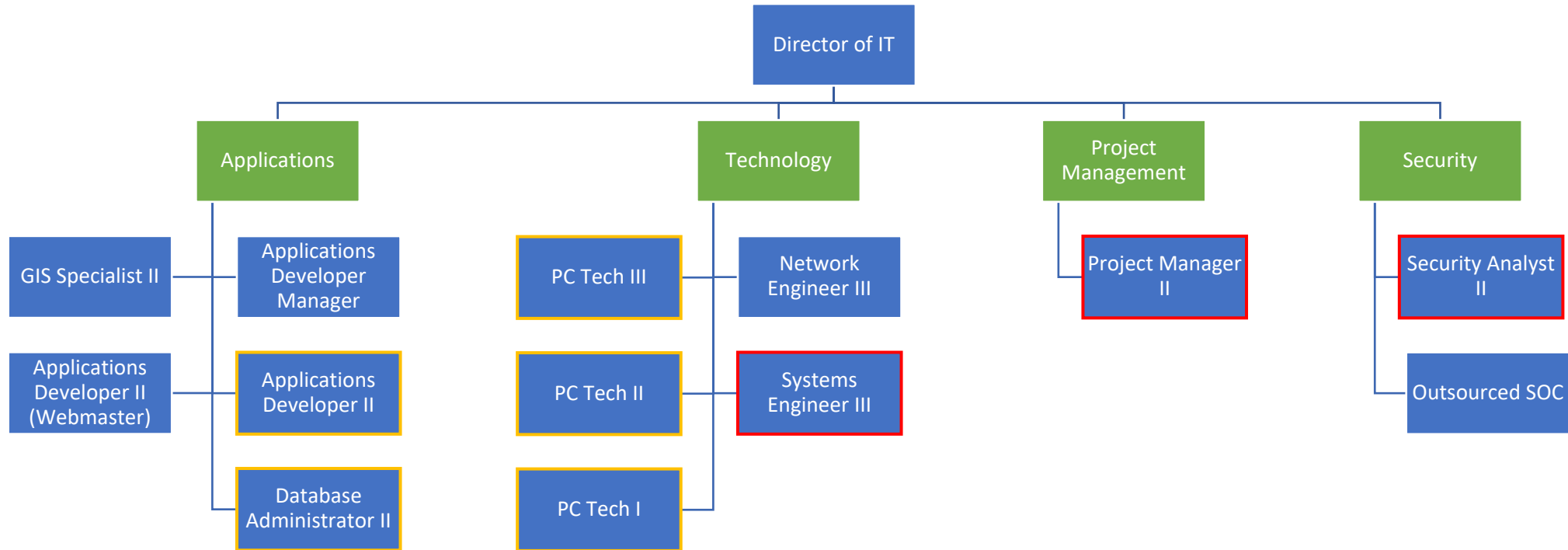
Timeline Overview



New Architecture



Recommended Organization Structure



LEGEND

YELLOW OUTLINE – CONVERTED CONTRACTOR
RED OUTLINE – NEW POSITION

Organization Costs

Current Role	Future Role	Current Cost	Future Cost	Delta
IT Manager	IT Director	\$178,481	\$210,820	(\$32,339)
Programmer Manager	Applications Development Manager	\$155,113	\$172,355	(\$17,242)
Webmaster	Applications Developer II	\$102,019	\$139,385	(\$37,366)
Sr. Programmer*	Applications Developer II	\$170,000	\$139,385	\$30,615
Sr. Programmer*	Database Administrator II	\$170,000	\$172,355	(\$2,355)
GIS Specialist	GIS Specialist II	\$107,954	\$107,954	---
Network Specialist	Network Engineer III	\$97,074	\$172,355	(\$75,281)
	Systems Engineer III	---	\$161,365	(\$161,365)
I.S. Technician*	PC Tech III	\$130,000	\$95,425	\$34,575
I.S. Technician*	PC Tech II	\$130,000	\$84,435	\$45,565
I.S. Technician*	PC Tech I	\$130,000	\$73,445	\$56,555
	Project Manager II	---	\$133,890	(\$133,890)
	Security Analyst II	---	\$144,880	(\$144,880)
			TOTAL DELTA	(\$437,408)

Next Steps

- What supporting documents would you need for City Council?
- Would you like us to support you in a meeting with City Council?
- Begin work on getting finalized proposals for your major agreements
 - The OKTA SSO component has the longest lead time and project timeline
 - Can we start negotiating with them right away and sign a contract in advance of the larger project approval?