City of Louisville, Colorado
Finance Department 749 Main Street Louisville CO 80027
(303) 335-4505 (phone) (303) 335-4506 (fax) www.ci.louisville.co.us

City Council
Finance Committee
Meeting Agenda
Monday, December 16, 2019
City Hall – Spruce Room
749 Main Street
3:00 p.m.

I. Call to Order
II. Roll Call
III. Approval of Agenda
IV. Approval of the Minutes from the November 22, 2019 Meeting (page 2)
V. Public Comments on Items Not on the Agenda
VI. I.T. Cybersecurity Update (page 7)
VII. Cigarette Tax Discussion (page 29)
VIII. Budget Calendar and Budget Process Discussion (page 33)
IX. 2020 Work Plan Review (page 37)
X. Staff Reports/Updates/Discussions
XI. Possible Discussion Items for Next Regular Meeting
   • Quarterly Reports
   • Continued Discussions on Budget Process
XII. Adjourn
CALL TO ORDER

The meeting was called to order at 9:30 a.m.

ROLL CALL

The following were present:

City Council: Council Member Maloney and Council Member Leh

Staff/Others Present: Heather Balser, City Manager, Emily Hogan, Assistant City Manager for Communications & Special Projects, Kevin Watson, Finance Director, Nathan Mosley, Director of Parks, Recreation & Open Space, Cara Golden, Accounting Manager, Penney Bolte, Tax Manager, and Nat Ahrens, IT Business Data Analyst

Absent: Council Member Lipton

APPROVAL OF THE AGENDA

Finance Committee Members approved the agenda as presented.

APPROVAL OF THE MINUTES FROM THE OCTOBER 25, 2019 MEETING

Finance Committee Members approved the October 25, 2019 minutes as presented.

PUBLIC COMMENTS ON ITEMS NOT ON THE AGENDA

None.
SALES TAX REPORTS FOR THE QUARTER ENDED SEPTEMBER 30, 2019

Tax Manager Penney Bolte presented the third quarter tax reports through September 30, 2019 to the Finance Committee. Manager Bolte stated that overall sales tax revenue, less any audit revenue, is trending up 4.8%, with in-City sales tax still holding at last year’s level, and out-of-City sales tax up 17%.

Finance Committee Member’s stated that, while the latest numbers were promising, they feel continuing with a more conservative approach is prudent for the time being. The Committee and staff discussed how analysis of the various trends should fit with any discussions of future business incentives.

The reports and corresponding narrative can be located in the packet of the November 22, 2019 Finance Committee Meeting.

REPROGRAMMING RECREATION SALES & USE TAX REFUND

Director Watson stated that at the November 5, 2019 election, voters approved the City retaining the full $845,800 collected in Recreation Sales & Use Tax and the continuation of the tax. Director Watson stated that the full $845,800 amount collected has already been used to fund the Recreation Center and Memory Square Pool operations, but an additional $845,800 of General Fund reserves was set aside pending the results of the election. Since voters approved the City’s retention of the revenue, these funds may now be reprogrammed or re-appropriated on an unrestricted basis.

Finance Committee Chairperson Maloney stated that he is interested in determining how to use the delta of the $845K collected and the $575K that was originally anticipated. Chairperson Maloney stated that it should be invested in a manner that supports the intent of the tax, and perhaps transferred to the Recreation Fund and used for projects that were value engineered out. Finance Director Watson and City Manager Balser stated that the General Fund appropriated and spent $1.5M for the Recreation/Senior Center and Memory Square construction, and that the $845K that was set aside could be left in the General Fund Reserves.

The Finance Committee requested staff bring forward a recommendation to the full City Council to include an accounting of what the funds were spent for.

The reports and corresponding narrative can be located in the packet of the November 22, 2019 Finance Committee Meeting.

REVIEW OF NON-PROFIT GRANT PROGRAM
Finance Director Watson presented a summary of the non-profit grant program to the Finance Committee stating that the appropriations for 2019 and 2020 were already determined, but that the Finance Committee had requested the process and funding for the 2021/2022 budget cycle be discussed. Director Watson also requested the Policy adopted by City Council September 5, 2017 for non-profit organizations (“NPO”) be discussed as this policy has not been followed for previous grant recipients.

Finance Committee Member Chris Leh stated that he was a member of the Legal Committee that drafted the NPO Policy, and that he sees some unintended consequences of the policy. The Committee and staff discussed the original intent of the policy and what types of entities it was designed to regulate, and whether or not the policy should apply to the applicants of the non-profit grant program. Of specific issue is the Policy’s requirement for the NPO to obtain a $1M liability policy.

The Committee and staff discussed whether the policy should be amended to provide a waiver for small non-profits not exceeding a certain level of funding, or if other amendments should be considered.

Finance Committee Member Maloney stated that he sees the grant program continuing as it is, or that the Policy adopted in 2017 needs to be reviewed by either City Council or the Legal Committee. Finance Committee Member Leh suggested the Policy be referred to the Legal Committee for City Attorney review to determine any risk in not following the Policy for the Non-Profit Grant Program or other possible revisions.

The reports and corresponding narrative can be located in the packet of the November 22, 2019 Finance Committee Meeting.

FINANCE COMMITTEE 2020 WORK PLAN

Finance Director Kevin Watson presented the current 2019 Finance Committee Work Plan for Finance Committee and staff discussion in setting the 2020 Work Plan. The Committee and staff noted that there were many one-time issue items in the 2019 Work Plan.

Finance Committee Chairperson Maloney stated that a full budget review may not be necessary for 2020, but large budget issues where the Finance Committee can be a value add for the full Council, should still be added to the 2020 Work Plan. City Manager Balser stated that a full budget process discussion is on the 2020 City Council Work Plan.

Chairperson Maloney stated that he would like to discuss the CIP budget process and forms at the December 2019 Finance Committee Meeting.
Parks, Recreation & Open Space Director Nathan Mosely requested the Finance Committee meetings be scheduled for later in the month to allow staff appropriate time to prepare the monthly dashboards. Finance Committee Member Leh requested the meetings also be held later in the day.

Finance Committee Chairperson Maloney stated that he and Finance Director Watson would work together on the 2020 Finance Committee Work Plan.

The reports and corresponding narrative can be located in the packet of the November 22, 2019 Finance Committee Meeting.

**STAFF REPORTS/UPDATES/DISCUSSIONS**

**Renewal & Replacement Worksheets**
Director Mosely stated the worksheets were being worked on and that staff needs time to perform a full inventory and develop a replacement schedule. Committee Members and staff determined the end of 1st Q or beginning of 2nd Q should be sufficient.

Director Mosely also stated that the RAB Committee will be meeting to discuss policies and guidelines for senior and youth program pricing, and asked that the review of the Recreation Center Fees and Rate Structure be delayed to late 1st or early 2nd quarter 2020.

**Other Staff/Committee Discussion**
Finance Committee Member Leh stated that he does not want City Council or the Finance Committee to drive any future KPI discussions. City Manager Balser stated that staff has issued an RFP for a consultant to assist to review the current KPI’s and processes, and to integrate them more fully into the City’s culture.

Member Leh also asked about discussions regarding the City’s Business Assistance Program. Chairperson Maloney stated that the process had been discussed by the Finance Committee and that several policies and processes were proposed but not yet implemented. City Manager Balser stated that once the new Economic Vitality Director is on board, discussions surrounding strategy, criteria, and the role of the newly formed Economic Vitality Committee will begin.

**DISCUSSION ITEMS FOR THE NEXT REGULAR MEETING**

The next regular Finance Committee Meeting is scheduled for Monday, December 16, 2019 at 3:00 p.m.

Items scheduled for discussion at the next meeting include:
- Budget/CIP Calendar, Process & Forms
- Work Plan
ADJOURN

The meeting was adjourned at 11:09 a.m.
SUBJECT: IT CYBERSECURITY UPDATE

DATE: DECEMBER 16, 2019

PRESENTED BY: CHRIS J. NEVES, IT DIRECTOR

SUMMARY:
The topic of cybersecurity is on everyone’s minds these days, especially in the public sector. The mainstream media are often reporting about another peer municipality, county or state agency succumbing to some type of security breach and falling prey to penetration by malicious hackers. Increasingly over the course of 2019 IT has been asked the question repeatedly, “What are we doing to keep our data safe?” In the paragraphs that follow, the intent is to answer that question in the most clear and concise summary possible. Attached is the most recent 2019 National League of Cities Cybersecurity report to help brief you on the topic.

City IT is following all the standard best practice protocols that are recommended to every organization, either public or private, to safeguard its systems. City IT relies heavily on open communication and end-user reporting to help address all these security challenges, as this is an organizational issue and not just a City IT concern. Cybersecurity vigilance and best practice are an organizational effort and the City will consistently hear this message in 2020.

In the fall of 2017 City IT engaged an independent outside security auditor, Istonish, to provide a comprehensive and objective assessment of IT security at the City. Since the City had undergone significant change in infrastructure and enterprise application systems between 2013 and 2017, in addition to several staff changes, IT needed this assessment as a baseline to its security efforts. At this time in 2019, the 2017 information is somewhat dated but provides a good foundational structure for IT to build on, which has already occurred. The report and findings that Istonish provided is highly confidential since it calls out specific vulnerabilities and the report includes privileged & proprietary documentation of the City infrastructure. The City scored pretty well and landed in the average range amongst similar sized organizations. The City did have some homework and remediation to do based on the findings. The City received the report in October 2017 and all recommended remedies were complete by the end of 2017.

City IT intends to undertake similar point-in-time security assessments every 4-6 years to get an independent perspective and re-assess baseline capabilities. In addition to these focused IT cybersecurity reviews, City IT is also annually audited by our financial auditors who ensure the City meets their PCI compliance and data standards for sensitive data.
Part of the IT Director role in the City is fostering and providing strong partnerships across neighboring peer cities and agencies and participating in regional, state and national consortiums. Cybersecurity is a topic that every IT resource has at the forefront of every decision they make and City IT is constantly gaining knowledge to be “in-the-know” through conversations and information sharing with other agencies. The City of Louisville is a member of MS-ISAC (https://www.cisecurity.org/ms-isac/) and https://www.CISecurity.org since 2016. These agencies work in partnership with the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The Colorado node of ISAC is very active and the City IT team engages regularly in their weekly communications and monthly briefings. MS-ISAC also provides free external scanning services. City IT has taken advantage of these services on an ongoing basis.

After the CDOT breach and other associated large breaches nation-wide, the cyber landscape of local and state governments changed quickly across the country. There is now a bigger emphasis on developing Cyber Event Incident Planning, up to and including provisions for the Governor to provide a State of Emergency declaration to enlist resources such as the National Guard and other federal agencies in these events. Louisville IT staff works hard to understand these issues and what resources are available should an event occur.

City IT is also a participating member in the Colorado Government Association of IT (CGAIT). Cybersecurity training is the number one topic during conferences. The IT Director is the current IT liaison to Colorado Municipal League (CML), and will be participating at the June 2020 Conference in Westminster on Cybersecurity. Lastly, over the last 3 years IT/Director has engaged with CompTIA/Public Technology Institute (PTI), whose job it is to keep current with State & Local CIOs across the country (and world) to provide relevant training and whitepapers on the ever-changing threat landscape. IT continues to consume as much knowledge as possible and focuses on keeping IT staff trained in relevant technologies.

Below are a few of the basic day-to-day operational tasks that City IT actively engages in for ongoing cybersecurity:

1. Staff training is the #1 defense to maintaining proper cybersecurity “hygiene”. Staff purchased a subscription to KnowBe4 (https://www.knowbe4.com/) this past summer. KnowBe4 is a cloud based security training and testing service. IT recently completed its first KnowBe4 campaign of internal phish testing. Out of 262 recipients targeted in its campaign, the City only had a “take rate” where someone clicked on bad content, 61 times. That makes the City 24.3% “phish prone”. Most agencies experience 40-50% “take rate” on their first campaign. The City’s goal is 0%, or at least very low single digits. The City will train all employees on how to avoid being “phished”. Staff will also provide some extra training for those that fail future targeted “phish” exercises. Cybersecurity threats are prevalent and vigilance needs to be maintained 24-7-365. IT is currently
working with Gloria in Communications and with HR staff to craft messaging and the training rollout for January 2020.

2. City IT has engaged MS-ISAC to run regular external scanning of the City’s public facing network to report any potential security anomalies or deficiencies.

3. City IT keeps all desktop and laptop system patches up-to-date. IT leverages a centralized console to make sure all City resources check-in and have the latest security patches. Servers receive patches on a rotational basis every Wednesday night.

4. All patron networks (Library, Recreation, Museum, etc.) are 100% isolated from the City network, including separate broadband. An event on the patron network would mean a shutdown of all patron computers and a restore through a program called reboot/restore. IT also keeps the patron network fully patched up-to-date and runs active Windows Defender antivirus on all patron computers. Patron computers are secured via local group policy security to minimize what users can do.

5. City IT actively monitors all network traffic, including WiFi networks, and all machines have limited permissions to perform installation or configuration changes without City IT’s involved and elevated permissions.

6. All staff read and acknowledge the City’s IT Security Policy. City IT staff also send out occasional emails when threat levels start ramping up. Training from KnowBe4 should enhance staff awareness to cybersecurity. IT encourages all employees to report events, not hide them.

7. City IT has hardened firewall filter policies and done maintenance to improve domain and email reputation to block malware at the perimeter and via email as much as possible without impeding work. All City computers patch frequently and run an enterprise class antivirus product. The City has had some “zero day” ransomeware events and they have been immediately isolated and contained with no impact on services. A “zero day” event is defined as an incident where the City is the first to be hit with something new and “unidentified” that is potentially destructive malware. Prior to running the City’s current product, the City did have 2 ransomeware encryption events within 6 months of each other in 2015 on their previous antivirus vendor. The City managed those events in 2015 with minimal operational impact due to our system backups, and without paying any type of ransom. No private data was impacted during those events. City IT learned a lot during those events. The City changed vendors at that time (2015) and increased knowledge and aptitude significantly.

8. City IT has a subscription to top-tier email SPAM filtering services. Based on that vendor’s current reporting, approximately 60% of all inbound email to the City is SPAM and is immediately quarantined or discarded. Again, 6 of every 10 inbound messages to City staff are SPAM. This percentage has been about the same since 2013. There are complaints about how aggressive the City’s SPAM filter is, but IT believes the current filtering is necessary. Staff can do more to educate in this area such as why the service is important, and what is blacklisting, whitelisting, etc.
9. IT has converted all firewalls to a top-tier application firewall vendor with intrusion
detection capabilities with active monitoring, logging and auditing. IT uses a
combination of standalone and firewall VPN for all remote sessions to internal
City resources.

10. City SCADA operations (Water, Wastewater) are also 100% isolated via firewall
from the City network and the Internet to ensure that integrity is maintained for all
water and wastewater services.

11. Most importantly, the City keeps up-to-date and regular backups of all systems
for disaster recovery and business continuity. Systems can be restored quickly to
within a few hours of a specific event.

Some future work plans related to cybersecurity that IT intend to move forward with in
2020:

1. A thorough inventory and assessment of PII data across our systems to
identify our data liabilities.

2. Create a cybersecurity Incident Plan (including a communication plan and
COOP assessment), and a cybersecurity Breach Plan (SB18-1128
compliance)

3. Staff is currently assessing and planning to move to Microsoft Office365 in
2020 to improve discovery and electronic retention.
   a. City Clerk Division will need to be included to discuss retention.
   b. Organizational process and procedural training will need to be a
      component of this effort.

4. Review current IT Security Policy and update policy & training to incorporate
KnowBe4 training.

5. Continue to improve upon Disaster Recovery and Continuity of Business
Operations Planning.

ATTACHMENTS:
Protecting Our Data:
What Cities Should Know About Cybersecurity
About the National League of Cities
The National League of Cities (NLC) is the nation’s leading advocacy organization devoted to strengthening and promoting cities as centers of opportunity, leadership and governance. Through its membership and partnerships with state municipal leagues, NLC serves as a resource and advocate for more than 19,000 cities and towns and more than 218 million Americans. NLC’s Center for City Solutions provides research and analysis on key topics and trends important to cities and creative solutions to improve the quality of life in communities.

About the Authors
Kyle Funk, Program Specialist of City Solutions
Cooper Martin, Director of Sustainability & Solutions
Nicole DuPuis, former manager of the Urban Innovation program at NLC’s Center for City Solutions
Alan Shark, the Executive Director and Dale Bowen is Managing Director, Public Technology Institute at CompTIA.

Acknowledgements
NLC is grateful for the guidance and review from the Public Technology Institute; Angelina Panettieri, Principal Associate for Technology and Communications, Federal Advocacy and John Manwell, Program Director for Information Technology at NLC; and Dan Lohrmann, Chief Security Officer & Chief Strategist at Security Mentor, Inc.

Table of Contents
3 Foreword
5 Introduction
7 What is Cybersecurity?
8 How Prepared are Cities?
15 Policy Landscape and Resources for Local Governments
18 Local Government Examples
21 Strategies and Recommendations for Local Leaders
25 Conclusion
27 References

2019 ©National League of Cities
All photo credited to Getty Images, 2019.
Foreword

Many of us remember a time before technology permeated every aspect of life - including our local governments. Not so long ago, our communities ran on filing cabinets stuffed with documents, fax machines and paper public transit schedules. Our timecards and records were kept by hand, and resident engagement only happened in-person or over the phone.

Today, our communities have moved online. This change has made many aspects of modern life more efficient. But this digital revolution is happening quickly, often at a pace faster than we can keep up with. As a result, individuals and institutions alike have been left vulnerable to hackers and ransomware.

Every day in the United States, a local government is hacked. Since 2013, ransomware attacks have impacted at least 170 county, city, or state government systems. The damage can cost millions, but the loss of public trust and safety come at an even higher price.

Despite being a primary target for hackers, local governments continue to integrate technology into their day-to-day operations and are increasingly collecting massive amounts of data. The pressure on cities to become “smarter” and more connected is mounting.

This rush toward digitization has resulted in a frenzy of competition and anxiety about being left behind, or not being able to provide the right services to their residents. As local leaders consider the risks and rewards of greater connection, they must also consider the crucial need for cybersecurity.

The National League of Cities remains committed to helping our members protect themselves, online and offline. That is why we are proud to release “Protecting Our Data: What Cities Should Know About Cybersecurity” in collaboration with the Public Technology Institute. This guide will help local leaders prepare and implement systems to protect their institutions online.

New technologies have the potential to create a brighter, more equitable future for the people in America’s cities, towns and villages. But, cybersecurity and smart city initiatives must go hand-in-hand. If we continuously invest in the people and systems needed to keep our information secure, our communities will thrive.

Clarence E. Anthony
CEO and Executive Director, NLC

The National League of Cities remains committed to helping our members protect themselves, online and offline.
Introduction

The White House reported that there were 77,200 cyber incidents in 2015 occurring in federal agencies alone. The Federal Trade Commission (FTC) received more than 800,000 consumer fraud and identity theft complaints, where consumers reported losses from fraud of more than $1.2 billion. Security threats from the “outside” are increasing in frequency and sophistication, but most of the greatest threats are coming from users “within” — network users who click on malicious links, open email attachments that contain viruses, or make other mistakes that allow hackers to gain access.

Public services are going digital. At the most complex level, this requires policymakers to understand, manage and regulate the use of facial recognition software and micromobility technology like e-scooters, energy storage, smart energy meters or autonomous vehicles. But data is also increasingly at the core of more fundamental services such as trash collection, building and zoning permitting, fleet management, public facility operations, utility maintenance and even tree inventories. The pressure on cities to become “smarter” or more connected is mounting, resulting in a frenzy of competition and anxiety about being left behind. A report from the McKinsey Global Institute estimates that the economic impact of the internet of things (IoT) in smart cities could surpass $1.7 trillion worldwide in 2025.1

Local governments do not often think of themselves as tech organizations, but nearly everything a government does depends on its ability to create, maintain and share large quantities of data — and to ensure that data is secure. Undoubtedly, the confluence of government and technology has great potential for cities to improve service quality and efficiency. But embracing technology-driven governance is not without risk.

Today’s networks are constantly being probed for weaknesses and vulnerabilities. All organizations must deal with these threats as technology continues to play a larger and larger role in business and governance. From Russia disrupting Ukraine’s infrastructure and breaches of corporations such as Equifax and Marriott, to attackers targeting American cities like Atlanta, Baltimore, and Riviera Beach, FL, ransomware and email scams plague internet users daily.

Local leaders should make cybersecurity an administrative and budgetary priority. When a local government is the victim of an attack, the cost can far exceed that of proactive investment in cybersecurity. In 2016, the average cost of a data breach was estimated to be about $6.53 million.2 However, in many cities, the cost can be even higher, and the price of failing to secure our networks is clearly rising. The cost for Atlanta to recover from its ransomware attack was estimated around $17 million.3 Similarly, the recent Baltimore ransomware attack is predicted to cost over $18 million.4

While there are several examples of high visibility hacks on the private sector, there are three main reasons why the concerns are very different when a local government falls victim to a breach:

- Governments collect and maintain far more sensitive information than most private sector companies.
- Residents can’t easily move or choose a competitor if they are unhappy with their local government service and security.
- Trust in government is eroding, and security breaches may further reduce faith in government.

Cybersecurity and smart city initiatives must go hand in hand as local leaders continue to invest in 21st century infrastructure. This municipal action guide is a collaboration of the National League of Cities and the Public Technology Institute. Our aim is to strengthen cybersecurity policies and systems in local governments. The guide looks at the state of cybersecurity in local governments and includes policy recommendations for local leaders to implement in order to keep their residents, and their own data, safe. To get a clearer picture of the state of cybersecurity in local governments today, NLC and PTI conducted a small survey of PTI’s IT members and NLC’s Information Technology Committee (ITC). We found that while local governments are making improvements, they still lack support from elected leaders and face budget constraints that limit their abilities to improve cybersecurity further.

There are many simple and effective steps cities can take to avoid vulnerabilities and reinforce cybersecurity best practices:

- Identify one individual to be responsible for cybersecurity programs in that jurisdiction
- Make digital hygiene an institutional priority
- Educate the local workforce, elected leaders and residents about cybersecurity
- Conduct an analysis of local government vulnerabilities
- Ensure your data is properly backed up
- Implement multi-factor authentication
- Create policies or plans to manage potential attacks
- Ensure public communication is part of your attack response plan
- Adopt a dot.gov (.gov) address to reduce risk of fraudulent municipal websites
- Work with educational partners to create a cybersecurity talent pool

No network can be 100 percent secure, but by following the recommendations in this guide, local government leaders can reduce the risk of a cyber-attack and be more resilient when one occurs.
When asked if the local government’s budget was adequate, 67 percent of respondents said it was high enough to secure the network properly. Over half of those who answered the survey said that elected officials tended not to prioritize cybersecurity budgets and policy.

NC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI sent the survey out to their broader membership while NLC targeted members of our Information, Technology and Communications Advocacy Committee, generating 165 responses:

45% represent communities with a population under 50,000
33% represent local governments in the 50,000 to 150,000 population range
22% represent local governments above 150,000 in population.

How Prepared are Cities?

How engaged are your local officials in cybersecurity efforts?
Only 17 percent of respondents say their local elected officials are very engaged in cybersecurity efforts. In fact, 29 percent admitted that they were “not engaged” at all.

Is your budget adequate enough to secure the network properly?
When asked if the local government’s budget was adequate, 67 percent of respondents said it was high enough to secure the network properly. Over half of those who answered the survey said that elected officials tended not to prioritize cybersecurity budgets and policy.
Protecting Our Data: What Cities Should Know About Cybersecurity

**DOES YOUR JURISDICTION PROVIDE FOR EMPLOYEE AWARENESS TRAINING (WHAT TO DO AND WHAT NOT TO DO WHEN IT COMES TO CYBER SECURITY)?**

Over three-fourths (75%) of local governments have a cybersecurity plan/strategy in case of an attack. These plans also include the steps to recover data should the system be breached.

- **Yes**: 76%
- **No**: 24%

**IF YOU HAVE A CYBERSECURITY PLAN, HOW OFTEN IS IT REVIEWED?**

- **Within the last two years**: 44%
- **Within the last year**: 22%
- **Within the last two years**: 7%
- **Never**: 3%
- **It has been more than two years**: 10%

**IF YES, WHAT IS THE FREQUENCY?**

- **Once a year**: 25%
- **Once every two years**: 44%
- **On-going/multiple times throughout the year**: 16%
- **Other (please specify)**: 10%

However, only 68 percent of these plans have been reviewed in the last year. This is troubling, since annual audits are considered a best practice with ever-changing technology and threats.

PTI and NLC’s survey revealed that around 76 percent of respondents conduct employee awareness trainings. While most (80%) conduct these trainings yearly, a few local governments only conduct cybersecurity training at employee onboarding.

The information collected by NLC and PTI are consistent with prior research and analyses in local government cybersecurity, indicating that little progress is being made to improve security in the face of mounting threats. In 2016, the International City/County Management Association (ICMA) and the University of Maryland, Baltimore County, conducted the first-ever survey of U.S. local governments about their cybersecurity practices and experiences. Their results revealed an alarming state of unawareness and unpreparedness for the majority of the 3,423 local governments they surveyed. These risks may cost local governments significant money and time as they seek to reverse the effects of a cybersecurity incident.

The most alarming result from the survey dispels the myth that cities, towns and villages are safe from attacks by bad actors. The survey found that 44 percent of local governments report an attack from a cyber incident hourly (26 percent) or daily (18 percent). That number rises to 66.7 percent over the duration of a year. But what is even more alarming is the large number of local governments that do not know how often they are attacked (27.6 percent), experience an incident (29.7 percent) or a breach (41.0 percent).

Worse still, while 88.8 percent of local governments know that most incidents come from external actors, nearly one-third (31.9 percent) do not know if the attacks were from an internal source or an external one. Even though local governments constantly experience incidents, a majority do not catalog or count attacks (53.6 percent).

According to the ICMA/University of Maryland, Baltimore County survey, local governments are trying to improve cybersecurity resilience through policy planning. The top policies that governments adopted included rules regarding how passwords are created, requirements on the frequency that end users must change their passwords and use of employee personal electronic devices on local government systems. Even though these policies were adopted, most officials incorrectly wrote them off as ineffective to increasing cybersecurity. The experts also noted in the paper that maintaining a strong cybersecurity culture with all users was vitally important. A strong cybersecurity culture means keeping good digital hygiene on top of mind, and sharing responsibility between all end users — not just the IT department or officials.

Though the ICMA/University of Maryland, Baltimore County survey revealed alarming cybersecurity results, the NLC/PTI survey shows that local governments are starting to adjust to the dangers the cyberworld presents. Three years have passed since the two surveys and cities, towns and villages seem to be progressing on cybersecurity. However, bad actors have not sat idly by. Nowadays, cybersecurity work will require constant evolution and local governments are best adapted to prepare and innovate solutions that can help the whole country remain secure.
Protecting Our Data: What Cities Should Know About Cybersecurity

**Does Your Local Government Outsource Any of Its Cybersecurity Functions?**

- 62% Do not outsource
- 30% Fully outsource
- 8% Partially outsource

(Graph courtesy of ICMA/University of Maryland, Baltimore County)

**Where Is the Primary Responsibly for Cybersecurity Located in Your Local Government’s Organization?**

- 89% Within the elected chief executive’s office
  - 5% Within the top appointed manager’s office
  - 2% Within the IT department or related unit
  - 1% Stand-alone cybersecurity department or unit
  - 3% Other department, unit, of office

(Graph courtesy of ICMA/University of Maryland, Baltimore County)

**If Outsourced, to What Office or Official in Your Local Government Does the Contractor(s) to Whom You Outsource Cybersecurity Report?**

- 50.3% IT Department
- 32.0% CIO or IT Director
- 13.1% Other Department
- 13.1% Top Appointed Manager’s Office
- 9.8% Chief Information Security Officer
- 4.6% Elected Chief Executive’s Office
- 2.6% Chief Technology Officer

(Graph courtesy of ICMA/University of Maryland, Baltimore County)

**To What Extent Is Each of the Following a Barrier for Your Local Government to Achieve the Highest Possible Level Cybersecurity?**

- Inability to pay competitive salaries for cybersecurity personnel: 50%
- Insufficient number of cybersecurity staff: 32%
- Lack of funds: 13.1%
- Lack of adequately trained cybersecurity personnel in my local government: 13.1%
- Lack of end user accountability: 9.8%

(Graph courtesy of ICMA/University of Maryland, Baltimore County)
Private Sector Perspectives:
6 STRATEGIES FOR CYBER SECURE CITIES
Haiyan Song, Senior VP and GM, Security Markets, Splunk

Cities are increasingly focused on cybersecurity best practices, with several high-profile attacks in recent years causing major disruptions to city operations across our nation. Developing the practices and tools to protect our cities from ransomware, cryptomining and a wide range of emerging threats is vital to safety, data protection and the security of the critical infrastructure that cities manage. But there’s hope in the chaos. The ability to dramatically improve your cybersecurity defense is within reach for the largest cities and smallest towns, provided we work together across all levels of government, academia and private sector partners.

Last fall I was honored to host a cybersecurity roundtable with the National League of Cities at Splunk’s San Francisco headquarters, where I shared advice from my years of conversations with cybersecurity experts around the globe in every industry. Here are some of our observations:

1. CITY LEADERS NEED TO UNDERSTAND THAT CYBERSECURITY ISN’T JUST AN IT DEPARTMENT CHALLENGE. It’s the responsibility of the entire organization, and the buck ultimately stops with leadership. In the private sector, there’s no question that cybersecurity is now a CEO and board-level responsibility, and recent cyber incidents for local governments have made it clear that mayors, city managers and councilmembers must be informed and ready to lead on this issue. City leaders need to align with their IT and security staff and stay informed about cyber risks and their potential impact to the city.

2. CITIES NEED TO START IMPROVING THEIR DEFENSES AND KEEP MOVING. There is no “finish line” when it comes to cybersecurity. It’s a continuous journey. No matter where your city is in its cybersecurity defense maturity, it’s important to commit to always moving forward. Threats are always evolving, which means your strategy to monitor, detect and act on risks must as well. Has your city adopted a risk-based cybersecurity framework, such as the one from the National Institute for Standards and Technology (NIST)? Does your city have a cyber incident response plan? If so, how often is it tested?

3. CYBERSECURITY IS A TEAM SPORT. Just as cities proactively form partnerships to prepare for natural disasters, it is critical that cities forge strong partnerships for cybersecurity incident response before disaster hits. Even the most technologically mature cities will struggle with resources if they are hit with a major cybersecurity incident. Cities must play an active role in sharing and collaborating with each other, other levels of government and security industry partners.

4. CITIES NEED TO UNDERSTAND THAT THE CYBERSECURITY TALENT GAP IS A GLOBAL PROBLEM WITH MILLIONS OF UNFILLED POSITIONS, and everyone is scrambling to recruit and train the next generation of cyber defenders. Do your local universities, community colleges or high schools have cybersecurity programs? Identify both short- and long-term talent pipelines for cybersecurity in your region. Be a champion of these programs and your cities will benefit.

5. BUDGETS ARE IMPORTANT. City IT leaders have been red flagging cybersecurity and the lack of an adequate budget as their top priority for years. Does your city have a dedicated cybersecurity budget? Is that budget realistic to provide the protection you’re aiming for?

6. LASTLY, THERE’S AN IMPORTANT QUESTION ALL LOCAL GOVERNMENTS SHOULD ASK: DOES YOUR IT LEADERSHIP HAVE ACCESS TO THE MODERN TOOLS IT NEEDS TO DO ITS JOB EFFECTIVELY? A modern cybersecurity practice fundamentally comes down to being smarter with data than those looking to do you harm or hold your data for ransom. Big data analytics, machine learning and even artificial intelligence (AI) aren’t futuristic fantasies, they’re the core technologies of today’s cybersecurity defenses.

It’s paramount that all city leaders look at security as a mission enabler and not just a checkbox. The most advanced cities I come across understand that data needs to be at the heart of any security operations center (SOC). And there’s a hidden pot of gold in putting advanced data analytics at the center of your security strategy. We’ve seen countless enterprises that learned the modern skills of being “data driven” through their cybersecurity practices, and then transformed their organizations by transferring those skills into their core missions. There are even examples of organizations taking the data skills and machine learning tools they use for cybersecurity and applying them to pressing policy issues like combating the opioid crisis and human trafficking.
Policy Landscape and Resources for Local Governments

Cities are not alone in this effort to secure public information. Several state governments are stepping up to assist cities as they identify areas of cybersecurity vulnerability. Local leaders should be aware of what their own state might offer, and advocate for programs that have been successful from other state governments.

Examples of this work can be found in Georgia and West Virginia, which are cultivating state government ecosystems to help cities improve their cybersecurity defenses. Georgia offers consultations to all municipalities upon request. They do this by creating IT contracts that allow them to work for local governments for general purpose or incident response needs. West Virginia has also followed this route, setting up state contracts to allow local governments to take advantage of state resources.

New York and Virginia are attempting to help local governments with different approaches. New York’s Department of Homeland Security and Emergency Services is helping local governments evaluate their vulnerability assessments against the Cybersecurity Framework developed by NIST. Virginia, on the other hand, is tackling cybersecurity with help from the military. The state has mobilized its National Guard to ‘State Active Duty’ status to perform vulnerability assessments and penetration tests on local government networks. The Commonwealth also plans to use homeland security grants to hold regional working group meetings on cybersecurity.

For any cybersecurity program to work, sharing costs and retaining talented cybersecurity employees in local governments is crucial. State officials in Michigan launched a chief information security office (CISO) service to aid nine small- and medium-sized governments. The program allows local governments to pay a fraction of the price for a trusted cybersecurity expert to assist them with their cybersecurity needs. CISO and other tech officials are engaged through this cost-sharing system which allows them to receive the expertise they normally could not afford on their own. This partnership approach resulted in improved cybersecurity for the state and was cited by FEMA as being a valuable example for other jurisdictions.

Dozens of state and local government agencies are members of the Multi-State Information Sharing & Analysis Center (MS-ISAC). This coalition is open and free for all state, local, tribal and territorial governments. MS-ISAC is hosted by the non-profit Center for internet Security and supported by the Department of Homeland Security, and provides multiple resources, including a 24/7 Security Operations Center, Incident Response Services and a Vulnerability Management Program.
Cyber Disruption Response Plans

Every government must be prepared to respond to cyber emergencies, in the same way that fire departments train and prepare to respond to fires. The National Governors Association (NGA) has created guidance on how to respond to emergency cybersecurity incidents. The NGA publication examines ‘Cyber Disruption Response Plans’ across America and offers best practices and tips to help. Bottom line, every government should test their processes and procedures with business leaders at least annually with a tabletop exercise that addresses cyber and other threats.


Local Government Examples

Durham, North Carolina
(228,330 population)

Durham, North Carolina, was hit with two major cyberattacks in the last decade. The first attack, in 2009, targeted the public-school system and multiple systems managing student grades. Phones and other networks were down for three months. Once the systems were back online, over 5,000 teachers had to manually reenter grades and other information. In addition to the costs of restoring or replacing hardware, the attack reduced functionality of the school system for months and it took thousands of hours to recover information.

Thus, the city of Durham worked diligently to create new policies, procedures and plans to make sure an attack like the 2009 incident never happened again. The school district and elected leaders established a cyber security framework complete with context, leadership, evaluation, compliance, audit, review and media plan. They also established partnerships with the FBI, the state of North Carolina and MS-ISAC.

When a second attack occurred in 2018, the city was better prepared. This time, the fleet vehicle network was inflicted with a virus that tried to jump to other agencies. DeWayne Kendall, deputy director of technology Solutions for the city of Durham, was worried.

“We were on our way to being in the newspaper,” he said.

When the second attack took place, staff quickly reached out to partners at MS-ISAC, who then connected them with staff in Allentown, Pennsylvania, who just had a similar attack. This time, instead of taking months to diagnose and identify the attack, they were able to do it in hours. The attack was shut down completely and the city was able to eliminate reinfections of the system within two weeks.

Worcester, Massachusetts
(Population estimate: 185,877)

The city of Worcester, Massachusetts, recognized that in order for its cybersecurity awareness program to be effective and successful, it must have support at the highest level. The city has increased its security efforts over the past year by prioritizing them in the fiscal 2019 budget, and creating a full-time data security specialist position to implement policies and procedures that will help safeguard the city’s data. The city also created a cybersecurity awareness trainer position, another full-time employee whose job was to deliver cybersecurity awareness training to employees on an ongoing basis. The city started its cybersecurity awareness program in October 2018.

Since cybersecurity is too broad of an area to tackle all at once, city officials identified training as the first priority. They aimed to train employees on cybersecurity awareness and equip them with the knowledge to help identify and prevent cybercrime. Additionally, the city continues to
research cybersecurity best practices and available training for local government. To date, the city’s cybersecurity awareness program includes:

A one-hour, mandatory introduction to cybersecurity awareness class to employees;

1. A process to encourage users to report suspicious emails;

2. Acknowledgment of “cyber champions” in each department who can help their co-workers identify “fake” emails, distribute awareness flyers and posters and participate in monthly meetings to provide input for additional cybersecurity awareness training;

3. Development and enforcement of security policies and


Cities interested in bolstering their approach to cybersecurity preparedness often start by seeking grant opportunities to help fund cybersecurity risk assessments. The city of Worcester received such funding to review current policies, processes and procedures and identify potential security risks.

Matanuska-Susitna Borough, Alaska
(Population around 100,000)

The Matanuska-Susitna Borough (Mat-Su) is a local government in Alaska with a population of about 103,000. Borough officials felt that they had a fairly secure system. The borough monitored web, email, and network traffic; weathered DDoS attacks, viruses, malware, and ransomware; and had a good backup/disaster recovery system designed to withstand the next big Alaska Earthquake.

In mid-2018, several local and state government organizations in Alaska were hit by cyber attacks. Matanuska-Susitna was hit with an advanced malware suite on July 23, 2018, that took down 150 servers and nearly 600 desktop computers. Mat-Su and the nearby city of Valdez were completely incapacitated. Both governments were infected with ransomware, but each responded differently. Valdez decided to pay the ransom, whereas Mat-Su did not. Upon investigation, Mat-Su found that the attack had infected and encrypted their backups. Primary cleanup and mitigation took three months and cost $2.5 million. To reduce the risk of a new infection, both locations completely rebuilt their networks and scrubbed all data imported to the new networks.

As for ransomware, the Mat-Su subscribes to the conventional wisdom of never paying a ransom, as doing so simply encourages the attacker to use new and bolder methods, and paying never guarantees a return of assets.

There are many models for cybersecurity, and the most common, prevention, is no longer enough. Since the attack, the municipality’s multi-level email filters capture more than 650,000 bad emails an hour, and yet there are still dozens of targeted email attacks that get through daily. For prevention to work, a city’s defense has to be correct 99 percent of the time, as no system will ever be perfect. Mat-Su now uses the detect and contain approach for that reason.

National League of Cities

The National League of Cities suffered a ransomware attack in February 2017. The total downtime experienced was less than 15 hours thanks to the inclusion of cybersecurity in NLC’s disaster recovery plan. By having, following and sticking to the plan, NLC was able to recover the stolen files without having to pay the ransom.

One evening, a network user noticed that several files were locked on the network drive and suspected that this was a potential ransomware attack. They immediately called NLC’s IT director who confirmed that the files were in a state of encryption caused by a ransomware attacker. The managed services provider (MSP) who maintains NLC’s network was contacted and quickly discovered the attack was coming from an account logged on through a terminal network that allows for remote working — essentially, the attacker was posing as an NLC employee. They immediately disconnected the user and reset the password to stop the hacker from getting back into the network.

By that time, over 11,000 files had been locked by the attack. However, there was no need to pay the ransom because NLC backs up its data every night. The first thing NLC’s disaster plan calls for is a recovery via a shadow copy from the off-site location to the on-site location, but this failed because of inadequate free space. A second action called for making the off-site file server the primary file server for the time being while the MSP took time to wipe clean and re-build the on-site server from scratch. Additionally, it was decided that terminal services be terminated during the recovery period and was later rebuilt.

There is nothing like an attack to test the disaster recovery plan for any government or organization, and NLC learned several important lessons about its strengths and vulnerabilities. First, the rapid response plan and nightly file backups allowed the organization to quickly respond to the initial attack. Second, hosting those backup copies off-site allowed the organization to quickly restore critical services after the attack, even while the primary file server was being rebuilt. Third, there were additional steps that the NLC could take to prevent similar attacks in the future. This included lengthening employee passwords to a minimum of 14 characters as suggested by the NIST security standard, adding an application to strengthen the terminal services by limiting the number of invalid login attempts, and implementing multi-factor authentication (MFA) on the terminal service and VPN. Finally, NLC made cybersecurity training mandatory for all staff with a focus on phishing and scams.
What Cities Need to Know About Cyber Insurance

As cyberattacks against local governments have become more widespread, cyber insurance has emerged as an attractive backup for some cities to expand the full set of cybersecurity protections. Insurance should not be considered an alternative to updating systems and improving digital hygiene, but no system can be 100% safe in such a dynamic and changing environment.

Cyber insurance premiums can cost thousands of dollars, but they can save a municipality much more, in the event that there is a cyberattack. Here are just a few things cities should include when thinking about the scope of potential coverage:

- Overtime for employees attempting to restore a system
- The cost of lost revenue (some non-recoverable)
- The cost of outside technical support services
- The monthly and annual costs to provide “free” credit monitoring reports to affected citizens or businesses whose information was stolen
- The replacement of some equipment
- Legal fees
- Forensics after an attack occurs
- Crisis management and post-event related expenses

WHAT DO CYBER INSURANCE COMPANIES LOOK FOR?

Some cyber insurance forms ask dozens of key questions. Failure to answer honestly could lead to a denial of payment. Imagine a chain smoker who smokes ten packs a day and falsely claims to be a non-smoker on a medical insurance form. Were the patient to succumb to a smoking-related illness, the insurance company is not obligated to pay anything. In the cyber realm, those providing cyber insurance want to minimize their risk as well, and premiums and deductibles are predicated on how good your jurisdiction manages its digital infrastructure. Common questions are:

- Has the jurisdiction adopted a cybersecurity incident response plan and adopted basic technology practices and policies?
- Are internet and email use policies reviewed with employees, elected leaders and contractors?
- Are employee access rights reviewed?
- How often is employee training provided and what is addressed?
- How are backups of devices managed?
- What anti-spam, anti-virus filters, anti-malware are utilized?
- Is computer access terminated when an employee departs?
- Is there an on-going process of forcing employees to change passwords?
- Are service providers required to demonstrate adequate security policies and procedures?
- What are the security and privacy provisions for cloud and managed services?
- What procedures are in place to test or audit your policies, procedures and controls?

PTI’s and NLC’s national survey of local government information technology officials revealed that 70 percent of respondents have cyber insurance. However, when asked what the amount of their insurance coverage was, 50 percent of respondents “did not know.” Whether known or not, the amount of coverage and exposure should be reviewed on a regular basis to make sure your organization is properly covered. While cyber insurance does not protect your municipality from a cyber-attack or breach, it does help to mitigate the risk that your municipality could be crippled indefinitely by an attack or faced with the prospect of having to front thousands of even millions of dollars in the wake of a cyber event. With this in mind, cyber insurance should be considered a key component of your government’s cybersecurity strategy.

Finally, be sure to reach out to your state municipal league to determine whether they offer cyber insurance through their affiliated risk pools.
Strategies and Recommendations for Local Leaders

1. **Identify one individual to be responsible for cybersecurity programs in that jurisdiction**
   This individual should be the “go-to” person when a security problem arises, and also serve as an “ambassador” who promotes cybersecurity awareness within the organization. With this role, they can also serve to enforce your cybersecurity rules and ensure staff receive the necessary training. They should report directly to the local government’s top executive/administrator. Larger municipalities should hire a full time IT executive. For smaller jurisdictions with tight resources, hiring a full-time IT person to help with more complex issues may not be possible. This is when local governments should consider soliciting state/county resources or partnering with a neighboring jurisdiction to address this need.

2. **Make digital hygiene an institutional priority**
   For local elected officials, keeping residents safe and secure is no longer just about having an able police force and sound justice system. Today, security encompasses the digital world and ensuring bad global actors cannot take advantage of weaknesses in online systems. Local leaders should work to promote a shift toward cybersecurity as a governing priority, both internally and in their connected communities. This should include emphasizing the importance of cybersecurity in the city budget, instituting best practices around cybersecurity and digital hygiene, recruiting new staff with cybersecurity and technical skills, training existing staff annually, training new staff as part of onboarding, and conducting an audit to identify points of weakness within local government networks.

3. **Educate the local workforce, elected leaders, and residents about cybersecurity**
   While investing in sophisticated software is important, towns and villages should invest heavily in people is also critical. NLC and PTI recommend that cybersecurity awareness training happen at least once a year, if not more. All new staff, including newly elected officials, should receive cybersecurity training as part of their onboarding processes. Lastly, periodic awareness campaigns should occur throughout the year. Be sure to also think what role city hall can play in reaching out to small and medium size business and schools. These places are also under constant attack. At the annual National Night Out in 2018, the city of Bellevue, Washington, created a venue for IT staff and community relations coordinators to meet with neighborhood groups, residents of low-income housing units and other local groups to inform parents and their children about online safety. The team plans to return next year and even started a monthly newsletter.

4. **Conduct an analysis of local government vulnerabilities**
   Before making any significant investments in cybersecurity systems or reinforcements, it is valuable to assess the gaps and weaknesses in your local government’s network. For

---

This is a rapidly changing landscape and there is an ongoing up-tick in attack vectors which make this a topic that cannot be ignored. Staff must know how to protect the enterprise systems and perimeter while balancing security and functionality. This requires an advanced, ever-evolving skillset and the ability to communicate and train end users rapidly. This is not just an IT problem, but an organizational one.

-Chris J. Neves, IT Director, City of Louisville, Colorado Information Technology
local governments, this might include identifying any vulnerabilities present in connected infrastructure throughout the city. Simple tabletop exercises for officials to practice their incident response plan can help identify these vulnerabilities, and many state governments can help coordinate these drills. As noted above, MS-ISAC is supported by the federal government to help local governments analyze and recommendations.

5. Ensure your data is properly backed up
The number one defense against ransomware is tested, offline (non-connected or cloud hosted) backups. This is an extension of good digital hygiene that is worth emphasizing for its own sake. Even organizations that have policy in place need to ensure that backups are being conducted frequently, that these backups are sufficiently isolated to avoid attack, and that they are technically capable of restoring service and functionality.

6. Implement multi-factor authentication
Multi-factor authentication (MFA) is a valuable tool against attacks. MFA requires a user to enter an additional security code or confirmation via their smartphone, e.g., through an app or text message. Cities should implement MFA on all business-critical systems, e.g., email. If an attacker gained the credentials of a city employee through a phishing attack, the attacker would still be blocked from gaining access because they don’t have their employee’s smartphone.

7. Create policies or plans to manage potential attacks
Every local government should have a cybersecurity response plan. This can be developed internally or with the help of a private sector firm that specializes in security. The plan should include several key components:

- Employee awareness training, incident response and after-action planning.
- An incident response team, similar to ones created to address natural or man-made disasters.
- Protocols to notify local law enforcement as well as other appropriate officials (state officials, the US Department of Homeland Security, FBI). Almost all states require that local governments contact the state CIO, the state attorney general, and other departments.
- Prioritization of systems to restore in case of an attack. For most governments this would mean making sure safety and health services come back online first or a shifting of resources if services cannot be brought back on immediately.

8. Ensure public communication is part of your attack response plan
Public trust is essential to local government, and when it comes to potential attacks, public communication is a unique concern. Utilize all of your jurisdiction’s communications channels to share information with the public – the press, social media, television. In the event of a data breach, some state laws require the local government to notify the press if a certain number of personally identifiable pieces of information are exposed.

What should you tell the public? Your community needs to know that their local leaders are fully engaged in the situation and are working to resolve it. To maintain the public trust, it is important to be as transparent as possible, keeping in mind that your jurisdiction is involved in a situation that impacts the public safety and full details may not be available until after the situation is resolved.

9. Consider converting to a dot gov (gov) domain
Hackers are not only attempting to target cities, they may impersonate a municipal service in order to target your residents. Identity thieves can easily create websites in the dot com (.com) or dot org (.org) domains that can look and seem like a legitimate web page and direct targets there to pay bills or submit personal information. These scams can be reduced by establishing your municipal systems on a .gov domain, which is much more difficult to mimic.

10. Work with education partners to create a cybersecurity talent pool
Individuals with cybersecurity skills are highly sought after in today’s job market, and the public sector often struggles to compete with the higher salaries in the private sector. Local leaders should tap into local community colleges, universities and high schools to help fill cybersecurity gaps. This way students can get hands-on experience and serve their communities, which may encourage to stay in in those positions. Two examples of this already exist. For twenty years, Cisco Networking Academy has worked to help students gain technical and entrepreneurial skills. Students can take courses online in subjects such as the IoT and cybersecurity. Along the way, Cisco will help students seek out job and networking opportunities. CompTIA is also working to create certifications around cybersecurity and keep those in the IT world on a growing path throughout their careers.
Today, digitization of services and management of sensitive data requires cities to invest in cybersecurity to fend off risks to their network. Local governments are in the midst of a sea of change, as more and more of their basic governance functions rely on technology. Connected infrastructure is critical to service delivery and efficiency.

Many improvements to local cybersecurity will involve partnerships between cities and private consultants or vendors who can provide important services. It is essential that local leaders understand that they can outsource many of these functions, but they cannot outsource responsibility. They have a duty to embrace cybersecurity both in practice and policy as tech is integrated into our cities, towns and villages. Local governments can prepare by doing the cyber basics and then begin stepping it up from there. Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care. The National League of Cities and the Public Technology Institute stand ready to help the nation’s local governments strengthen their cybersecurity efforts.

Conclusion

Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care.
Protecting Our Data: What Cities Should Know About Cybersecurity

References

NLC/PTI Survey: NLC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI sent the survey out to their members while NLC sent the survey out to its ITC Committee. With 165 responses 45 percent represent communities with a population under 50,000, 33 percent represent local governments in the 50,000 to 150,000 population range while 22 percent represent local governments above 150,000 in population.

Label Resources


Cybersecurity And The Rise Of Smart City Vulnerability (Smart Resilient Cities) https://www.smartresilient.com/cybersecurity-and-rise-smart-city-vulnerability

Cybersecurity: Protecting Local Government Digital Resources (Corey Fleming and all. ICMA and Microsoft, May 2017).

Cybersecurity Challenges to American Local Governments (Donald F. Norris et al., UMBIC) https://etbiquity.umbc.edu/_file_directory_/papers/874.pdf


MS-ISAC https://www.cisecurity.org/ms-isac/

National Cybersecurity Preparedness Consortium http://nationalcpc.org/

National Cyber Security Alliance https://staysafeonline.org/


End Notes


6. Ibid.


8. Ibid.

9. Ibid.


Appendix A: Cybersecurity Checklist

The following is a comprehensive checklist to determine the level of security controls within your city. This checklist was adapted from a resource developed by James E. Piscanekowski II, CGOO, Ventnor City, NJ.

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have policies and procedures to address authorized and limited access to facilities, including data centers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are visitors escorted in and out of controlled areas?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are PC screens automatically locked after an idle period?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies covering laptop, tablet, or mobile device security?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a current emergency evacuation plan?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have an accurate up to date inventory of all electronic equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your data closets and/or server rooms equipped with intrusion alarms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your data center/server room locked at all times?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have environmental controls dedicated to your data closets and server rooms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have fire suppression systems dedicated to your data closets and server rooms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are default security settings changed on software and hardware before they are placed in operation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures in place to control equipment plugged into the network?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your physical facility monitored and reviewed via camera systems?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Totals

End Notes

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have policies and procedures to address authorized and limited access to facilities, including data centers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are visitors escorted in and out of controlled areas?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are PC screens automatically locked after an idle period?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies covering laptop, tablet, or mobile device security?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a current emergency evacuation plan?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have an accurate up to date inventory of all electronic equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your data closets and/or server rooms equipped with intrusion alarms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your data center/server room locked at all times?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have environmental controls dedicated to your data closets and server rooms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have fire suppression systems dedicated to your data closets and server rooms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are default security settings changed on software and hardware before they are placed in operation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures in place to control equipment plugged into the network?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your physical facility monitored and reviewed via camera systems?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix A: Cybersecurity Checklist

### Personnel

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your staff wear ID badges?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you check credentials of external contractors?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies to address background checks of contractors?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies addressing background checks of employees?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a policy for unauthorized use of “open” computers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a policy and procedure in place to handle the removal of employees who retire, are terminated, or leave, including passwords and access to systems?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have an acceptable use policy that governs email and internet access?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a policy governing social media use and access by employees?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are employees required to sign an agreement verifying they have read and understood all policies and procedures?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are these policies and procedures reviewed by employees at least annually?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Totals**

### Account and Password Management

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have policies and procedures covering authentication, authorization, and access control of personnel and resources to systems?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies in place to ensure only authorized users have access to PCs?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures in place to enforce secure, appropriate, and complex passwords?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are information systems such as servers, routers, and switches protected with basic or better authentication mechanism?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the default “Administrator” account been disabled and/or deactivated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all access attempts logged and reviewed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are employees required to change their passwords on a routine schedule?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are employees prevented from using previous passwords?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all passwords on network devices encrypted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have legal and/or policy notifications on all log-in screens that is seen and accepted prior to access to any network device?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Totals**

### Data Security

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have policy for information retention?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies and procedures for management of personal private information?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a policy for disposing of old and outdated equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies and procedures in place for the secure destruction or sanitation of media and/or drives before they are removed, sold, or disposed of?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is access to data or systems accessed remotely both from a dedicated link and encrypted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have policies and procedures in place to ensure that documents are converted into formats that cannot be easily modified before they are circulated outside the network?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are documents digitally signed when they are converted to formats that cannot be easily modified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is access to critical applications restricted to only those who need access?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are UPS batteries used on all critical equipment?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Totals**

---

NATIONAL LEAGUE OF CITIES

Protecting Our Data: What Cities Should Know About Cybersecurity

Appendix A: Cybersecurity Checklist

NATIONAL LEAGUE OF CITIES
### Network Security

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is network traffic regularly monitored for patterns?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do critical systems have redundant communication connections?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your network utilize redundant DNS servers in case of interruption to one server?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your DNS servers reviewed on a periodic basis for anomalies and consistency?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your Active Directory reviewed periodically for anomalies and consistency?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all unnecessary services disabled on servers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your network utilize redundant domain controllers in case of interruption to one server?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there policies and procedures governing the use of wireless connections to your network?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are wired and wireless networks within your organization segregated either physically or virtually through routers, switches, or firewalls?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you employ firewalls on your network to control access and traffic?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are firewalls configured to only allow traffic from approved lists?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are network security logs reviewed regularly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are web filters used to restrict downloading of unapproved material?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are filters or firewalls used to filter executable or malicious email attachments?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures in place for software patches and updates?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures in place for hardware patches and updates?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your security policies reviewed on a yearly basis?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are current and up to date antivirus solutions loaded on all computers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are antivirus and other security software updated with current patches on a regular basis?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you use spyware and malware detection software?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all computers current with all security and operating system patches and updates?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you use employee “least privilege” access and review access privilege periodically?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have an accurate and up to date software inventory list?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Totals | 28 |

---

*Network Security* refers to the measures taken to ensure the security of a network. This includes monitoring for patterns, having redundant communication connections, reviewing DNS servers,Active Directory, and network security logs, disabling unnecessary services, using firewalls, web filters, and antivirus software, and ensuring up-to-date security policies and inventory.
SUBJECT: CIGARETTE TAX DISCUSSION

DATE: DECEMBER 16, 2019

PRESENTED BY: PENNEY BOLTE, FINANCE DEPARTMENT

SUMMARY:

Background:
Beginning in 1964, the State of Colorado levied a 1¢ per cigarette excise tax. Wholesalers are responsible for the collection and remittance of the excise tax to the Colorado Department of Revenue.

In 1973, House Bill 1973-1492 allowed for the distribution of 27% of the State Cigarette Tax (excise tax) to cities, towns, and counties. At that time, the State Cigarette Tax was 20¢/pack. This “share-back” was conditioned upon no local sales tax imposition on cigarettes, and was apportioned based on State sales tax collections for Louisville-sourced sales as a percentage of total State sales tax collections.

In 2004, Colorado voters approved Amendment 35, which added 64¢/pack for specified health programs, bringing the combined State Cigarette Tax to 84¢/pack.

On July 1, 2009, as a result of passage of HB 09-1342, the State lifted its former sales tax exemption and started imposing its 2.9% sales tax on the retail sale of cigarettes for the period July 1, 2009 to June 30, 2011. This imposition of sales tax was later made permanent. State statutes still prohibited all local municipalities from lifting their own sales tax exemptions on cigarettes, unless a measure was put to voters and the municipality forfeited its share-back portion of the State Cigarette Tax.

Recent Changes in Legislation:
Most recently, HB19-1033 was enacted July 1, 2019. This bill permits local municipalities (statutory and home-rule) to impose fees and licenses on cigarette sales without forfeiting their share of the State Cigarette Tax. The bill also authorizes a county or city to adopt its own special sales tax upon all sales of cigarettes, tobacco products, or nicotine products, provided any such proposal is referred to and approved by the voters in such municipality. If such special tax is approved, the municipality would forfeit its share of the State Cigarette Tax.

This most recent revision to the Colorado Revised Statutes has spurred a great deal of discussion among home-rule cities. A preliminary survey among home-rule cities indicates some cities are evaluating a special sales tax (Glenwood Springs, Arvada, Aurora, and Wheat Ridge), while others (Denver, Golden, Commerce City, Littleton, and Steamboat Springs), have no plans for a special sales tax.
There are other elements to HB19-1033 that should be considered. State statutes have also been revised such that a county could impose a special sales tax in each municipality within its jurisdiction, in whole or in part. The bill states, provided a city within its county has not adopted its own special sales tax, the county may levy, collect, enforce and administer a county special sales tax upon all sales of cigarettes, tobacco products, or nicotine products of such city.

Counties would be responsible to obtain voter approval within their county and would also be responsible to collect and administer the special sales tax. The Colorado Department of Revenue, which currently collects and administers sales tax for all but two Colorado counties, would not be responsible to collect a special sales tax on cigarettes, tobacco or nicotine products.

Should a city adopt its own special sales tax after such county, the county would need to enter into a mutually acceptable intergovernmental agreement (IGA) with the city to either continue to assess its full special sales tax, or for the apportionment of a specified percentage of the gross county special tax revenue collected by the county to the municipality. Absent such IGA the county special sales tax would be forfeited in full.

**Sales Tax vs. Special Sales Tax:**
State statutes define a “special sales tax” as a tax imposed by a local government that is separate from a general sales tax imposed, and may be imposed in addition to those taxes.

This means a couple things. For one, the City of Louisville could not “lift” its exemption for cigarettes from the imposition of our standard sales tax (3.65%) and begin collecting sales tax on cigarettes. A separate “special sales tax” would need to be approved by voters.

The City of Louisville currently exempts “cigarettes” only, from its standard sales tax. All other tobacco (cigars, pipe tobacco) and nicotine products (E-cigarettes, nicotine cartridges) are currently subject to the City’s standard sales tax.

If a special sales tax was proposed and approved, however, the above tobacco and nicotine products currently taxed under our standard sales tax rate, would additionally be subject to the special sales tax. This would result in cigarettes taxed at the special sales tax rate only, but all other tobacco and nicotine products taxed at the standard sales tax rate and the special sales tax rate. It may be possible, as part of any proposal referred to voters, for all tobacco and nicotine products to be excluded from the City’s standard sales tax and placed under the provisions of the newly proposed special sales tax, thus creating one special sales tax rate for all cigarettes, tobacco and nicotine products.

**Louisville Statistics:**
It is estimated that retailers in the City of Louisville sell between $1.8 - $2.2 million dollars of cigarettes each year. This number includes sales made by grocery, convenience, and
liquor stores, as well as other licensed retailers. The (3) convenience stores sell the largest overall percentage of cigarettes at 51%, followed by (8) grocery/liquor stores at 37%, and the remaining other licensed retailers at 12%.

In relation to total retail sales for the above businesses, cigarettes comprise 7%-9% of total sales for convenience stores, 1.5%-4% for liquor stores, less than 1% for grocery stores, and 2%-7% for other retailers. The volume of sales of other tobacco or nicotine products is unknown at this time, as those sales are reported as part of the total retail sales made by the retailer.

To provide an example, and based on sales estimates solely for cigarettes, imposing a “special sales tax” rate equal to our standard sales tax rate (3.65%) would generate $65K - $80K in tax annually. Louisville currently receives approximately $40,000 annually as its share-back allotment of the State Cigarette Tax. The allocation percentage is based on the total sales tax revenue collected by the State for Louisville-sourced sales as compared to total State sales tax collection for all political subdivisions. Louisville’s current allocation is 0.00343%. Municipalities do not receive any portion of the federal excise tax on cigarettes, nor any portion of the state sales tax imposed by HB 09-1342.

Consideration/Discussion:

1. Do nothing. Continue to exempt cigarette sales from our standard sales tax and collect State Cigarette Tax allocation.
   a. Cities that elect to impose a special sales tax will not be included in State allocation.
   b. Fluctuations may occur with the cigarette share-back amount for Louisville due to:
      i. The amount of State sales tax revenue increase remitted by remote sellers
      ii. The unknown percentage of remote seller sales tax attributable to Louisville-sourced sales
      iii. Increases or decreases in overall cigarette sales in the State affecting the amount of revenue in the share-back pool

2. Implement Licensing & Enforcement Program. Establish licensing and compliance regulations for retailers of cigarettes, tobacco or nicotine products. Legislation would have to be approved by Council for inclusion in the Municipal Code to create such a program.
   a. City may retain its allocation of the State Cigarette Tax share-back.
   b. It is estimated the City of Louisville has (14) establishments that sell tobacco and nicotine products.
   c. License fees may cover only the costs of administering the licensing program and enforcing tobacco retail policies. Average national occupational license fees in the U.S. range from $50-$500 per establishment, per year.
d. Much of a program such as this would still need to be determined, however staff assumes enforcement provisions of the licensing code would be handled by the Police Department and Local Licensing Authority similarly as to how liquor and marijuana violations are handled. Violations would put the licensee at risk of a license suspension, fee in lieu of license suspension, or license revocation.

e. If the Council is interested in making changes this may allow the Council to determine maximum number of licenses permitted in the City, or address other zoning matters through new legislation.

3. Propose a special sales tax on all retail sales of cigarettes, tobacco and nicotine products within the City of Louisville.
   a. Requires a measure be referred to voters for approval and the related election costs.
   b. Forfeit of State Cigarette Tax share-back allocation.
   c. The revenue from any such special sales tax may be used for any purpose determined by the governmental body.
   d. May enter into an intergovernmental agreement with Boulder County should Boulder County enact a special sales tax before the City of Louisville to:
      i. Allow the County to continue collecting its full special sales tax rate even after the City begins imposing its special sales tax.
      ii. Allow the County to continue collecting its full special sales tax rate even after the City begins imposing its special sales tax, but negotiate a provision for the apportionment of a specified percentage of the gross county cigarettes, tobacco, and nicotine products special sales tax to the City.
   e. Not allow the County to continue collecting its special sales tax once the City’s special sales tax collection begins.
   f. Costs associated with creating new tax remittance forms and updating tax software.
FINANCE COMMITTEE COMMUNICATION

SUBJECT: BUDGET CALENDAR AND BUDGET PROCESS DISCUSSION

DATE: DECEMBER 16, 2019

PRESENTED BY: KEVIN WATSON, FINANCE DIRECTOR

SUMMARY:

The City’s 2021-2022 biennial budget process will begin in January 2020. Attached is a draft of the 2021-2022 Biennial Budget Development Calendar. This is a preliminary draft that will be presented to the Department Directors at the December 17 Management Team Meeting.

Also attached is a draft of the 2021-2026 Capital Improvement Plan Request form, which will also be presented at the December 17 Management Team Meeting. This form has various communication purposes:

- Communicate the dollar amount of the request by Program, Sub-Program, Fund, and year to the Finance Department;
- Communicate any offsetting revenue and the impact to operations to the City Manager and Finance Department;
- Communicate a general description, justification, and project timing of the project to the City Council and City Manager; and
- Since a copy of the form will be included in the published budget document, inform the public as to the key elements of the project.

Staff anticipates the Tyler-Munis ERP system will be used for the majority of operational requests. Finance staff will develop separate request forms for new positions, non-benefitted part-time hours, and overtime.

Staff requests the Committee review the Budget Calendar and Request for C-I-P form and let staff know of any changes to these or to the overall budget process.
<table>
<thead>
<tr>
<th>Dates</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 20, 2020</td>
<td>Finance Issues Instructions and Forms to Departments for Six-Year Capital Improvement Plan Requests</td>
</tr>
<tr>
<td>February 3 - March 27, 2020</td>
<td>Department Liaisons Request Input and Recommendations on Operating &amp; Capital Budget from Advisory Boards</td>
</tr>
<tr>
<td>February 5 - March 27, 2020</td>
<td>Departments Prepare Requests for Six-Year Capital Improvement Plan</td>
</tr>
<tr>
<td>March 23, 2020</td>
<td>Finance Presents to Departments Current-Year Budget Amendment Worksheet for Rollovers, New Items, Etc.</td>
</tr>
<tr>
<td>March 23 - April 3, 2020</td>
<td>Departments Prepare Requests for Six-Year Capital Improvement Plan Amendments</td>
</tr>
<tr>
<td>March 27, 2020</td>
<td>Departments Submit Requests for Six-Year Capital Improvement Plan</td>
</tr>
<tr>
<td>March 30 - May 1, 2020</td>
<td>Finance Consolidates and Summarizes All Requests for the Six-Year Capital Improvement Plan</td>
</tr>
<tr>
<td>April 3, 2020</td>
<td>Departments Submit Completed Budget Amendment Worksheets or Other Documentation to Finance</td>
</tr>
<tr>
<td>April 6 - April 24, 2020</td>
<td>Finance Prepares Preliminary Current-Year Budget Amendment for Rollovers, New Items, and Revenue Adjustments</td>
</tr>
<tr>
<td>April 24, 2020</td>
<td>Finance Issues Council Communication to Departments for Narratives on Current-Year Budget Amendment</td>
</tr>
<tr>
<td>April 27 - May 8, 2020</td>
<td>Departments Review and Verify Preliminary Current-Year Budget Amendment and Prepare Narratives</td>
</tr>
<tr>
<td>May 1, 2020</td>
<td>Finance Submits Consolidated C-I-P Requests and Fiscal Impact Summary to City Manager</td>
</tr>
<tr>
<td>May 4 - May 22, 2020</td>
<td>City Manager Reviews Requests for Six-Year Capital Improvement Plan Amendments</td>
</tr>
<tr>
<td>May 8, 2020</td>
<td>Departments Submit to Finance Final Changes and Narratives for Current-Year Budget Amendments</td>
</tr>
<tr>
<td>May 11 - May 22, 2020</td>
<td>Finance Consolidates Department Narratives and Makes Final Changes to Current-Year Budget Amendment</td>
</tr>
<tr>
<td>May 15, 2020</td>
<td>C-I-P Retreat: City Manager Meets with Departments and Reviews Requests for Six-Year Capital Improvements Plan</td>
</tr>
<tr>
<td>May 18 - May 29, 2020</td>
<td>Training for Department Representatives on Updating Operational Budgets into Tyler</td>
</tr>
<tr>
<td>May 22, 2020</td>
<td>City Manager Issues Initial Recommendations on the Six-Year Capital Improvements Plan</td>
</tr>
<tr>
<td>May 25, 2020</td>
<td>Finance Submits Final Current-Year Budget Amendment for Council Adoption</td>
</tr>
<tr>
<td>May 25 - June 6, 2020</td>
<td>Finance Consolidates and Summarizes City Manager's Recommendations on the Six-Year C-I-P</td>
</tr>
<tr>
<td>June 1, 2020</td>
<td>Finance Issues Instructions and Personnel Request Forms to Departments for Requesting Operational Budgets</td>
</tr>
<tr>
<td>June 1, 2020</td>
<td>Finance Issues Forms to Departments for Six-Year Revenue Estimates</td>
</tr>
<tr>
<td>June 1 - June 12, 2020</td>
<td>Departments Review Employee Cost Allocations and Submit Changes to Human Resources</td>
</tr>
<tr>
<td>June 1 - June 19, 2020</td>
<td>Departments Prepare Six-Year Revenue Estimates for All Revenue Collected or Assessed by Departments</td>
</tr>
<tr>
<td>June 1 - June 28, 2020</td>
<td>Departments Input Biennial Operating Budget Requests Into Tyler and Complete Personnel Request Forms</td>
</tr>
<tr>
<td>June 2, 2020</td>
<td>City Council Considers Current-Year Budget Amendment for Rollovers, New Expenditure Items, &amp; Revenue</td>
</tr>
<tr>
<td>June 8, 2020</td>
<td>Finance Submits Preliminary Recommended C-I-P Document with Fiscal Impact to City Manager and Departments</td>
</tr>
<tr>
<td>June 12, 2020</td>
<td>Finance Department Issues Letters and Application Forms to Non-Profit Agencies for Non-Profit Grant Program</td>
</tr>
<tr>
<td>June 19, 2020</td>
<td>Departments Submit Revenue Estimates to Finance for All Revenue Assessed or Collected by Departments</td>
</tr>
<tr>
<td>June 26, 2020</td>
<td>Departments Complete Input of Biennial Operating Budget Requests and Submit Personnel Requests to Finance</td>
</tr>
<tr>
<td>Dates</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>June 29 - July 10, 2020</td>
<td>Finance and Human Resources Prepare First Draft of Wage &amp; Benefit Projections (Requested Budget)</td>
</tr>
<tr>
<td>June 29 - July 31, 2020</td>
<td>Finance and Human Resources Prepare Biennial Operating Requests and Consolidates Financial Impacts</td>
</tr>
<tr>
<td>July 6 - July 31, 2020</td>
<td>Departments Compile Annual Key Performance Indicator Updates</td>
</tr>
<tr>
<td>July 17, 2020</td>
<td>City Council Budget Retreat: Prior Year Review, Current Year Revenue Updates, C-I-P Review, LTFP Review</td>
</tr>
<tr>
<td>July 31, 2020</td>
<td>Finance Submits Consolidated Biennial Budget with Fiscal Impacts to City Manager &amp; Departments</td>
</tr>
<tr>
<td>July 31, 2020</td>
<td>Departments Submit Updated Annual Key Performance Indicators to City Manager</td>
</tr>
<tr>
<td>August 3 - August 14, 2020</td>
<td>City Manager Reviews Operational Budget Requests and Meets with Departments</td>
</tr>
<tr>
<td>August 14, 2020</td>
<td>City Manager Relays Final Decisions to Finance and Departments on Recommended Budget</td>
</tr>
<tr>
<td>August 17 - August 28, 2020</td>
<td>Finance and Human Resources Prepare Second Draft of Wage &amp; Benefit Projections (Recommended Budget)</td>
</tr>
<tr>
<td>August 17 - September 4, 2020</td>
<td>Finance and Human Resources Prepare Consolidated Recommended Budget - Prepares for Distribution</td>
</tr>
<tr>
<td>September 7, 2020</td>
<td>Non-Profit Agencies Submit Grant Request Applications to Finance Department</td>
</tr>
<tr>
<td>September 15, 2020</td>
<td>City Manager’s Recommended Budget Presented to City Council at a Regular Meeting (Public Hearing Set)</td>
</tr>
<tr>
<td>September 22, 2020</td>
<td>City Council Reviews and Discusses Recommended Budget at Study Session (Special Meeting)</td>
</tr>
<tr>
<td>September 23 - October 9, 2020</td>
<td>Finance Consolidates and Summarizes a Revised Recommended Budget for Public Hearing and Distribution</td>
</tr>
<tr>
<td>September 23 - October 20, 2020</td>
<td>Finance and Human Resources Prepare Final Wage &amp; Benefit Projections (Revised Recommended Budget)</td>
</tr>
<tr>
<td>October 16, 2020</td>
<td>Finance Prepares and Issues Public Notice for October 20 Public Hearing (Publish October 16)</td>
</tr>
<tr>
<td>October 20, 2020</td>
<td>City Council Conducts Public Hearing on Revised Recommended Budget</td>
</tr>
<tr>
<td>October 27, 2020</td>
<td>City Council Reviews and Discusses Revised Recommended Budget (Final Meeting before Adoption)</td>
</tr>
<tr>
<td>October 28 - November 8, 2020</td>
<td>Finance Prepares Final Budget and Resolutions to Adopt the Budget, Appropriate Funds, and Levy Taxes</td>
</tr>
<tr>
<td>November 17, 2020</td>
<td>City Council Presented with Resolutions to Adopt the Budget, Appropriate Funds, and Levy Taxes</td>
</tr>
<tr>
<td>November 18, 2020</td>
<td>Finance Prepares Mill Levy Certification Letter and Submits to City Clerk for Signature and to Boulder County</td>
</tr>
<tr>
<td>November 18 - December 31, 2020</td>
<td>Finance Prepares Formal Budget Document and Application to GFOA for Budget Presentation Award</td>
</tr>
<tr>
<td>December 15, 2020</td>
<td>City Council is Presented with Finance Committee Recommendations on Non-Profit Agency Grants</td>
</tr>
<tr>
<td>January 2, 2021</td>
<td>Finance Publishes Formal Budget Document and Submits Application to GFOA for Budget Award</td>
</tr>
</tbody>
</table>

City Manager & Council
City Manager
All Departments
Finance & Human Resources
Finance Department

Dated: 12/06/19
Six-Year (2021-2026) Capital Improvement Plan
Request Form for Capital Equipment or Capital Project

Identification and Funding Source

<table>
<thead>
<tr>
<th>Program(s):</th>
<th>Sub-Program(s):</th>
<th>Funding Source(s):</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Submitted By: ___________________________ Version: ___________________________

Identification and Funding Source

- Project Name: ___________________________
- Program(s): ___________________________
- Sub-Program(s): _______________________
- Funding Source(s): ____________________
- Percent: ______________________________

Estimated Cash Flow Schedule

<table>
<thead>
<tr>
<th>Equipment or Project Costs</th>
<th>Year 1 2021</th>
<th>Year 2 2022</th>
<th>Year 3 2023</th>
<th>Year 4 2024</th>
<th>Year 5 2025</th>
<th>Year 6 2026</th>
<th>Six-Year Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land Acquisition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design &amp; Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Prof Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Equip/Project Costs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capital Equipment Purch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Costs (Gross)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grants or Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Off-Setting Revenue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact to Annual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maint/Operating Costs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description and Justification

Description & Proposed Funding:

Equipment/Project Description:

Narrative ...

Project revenue or grants, if any, that will support the project and the impacts to the operating budget:

Narrative ...

Justification and Alignment with Program/Sub-Program Goals & Key Performance Indicators:

Narrative ...

Department Priority Ranking: ___________________________ Request Number: ___________________________
SUBJECT: FINANCE COMMITTEE 2020 WORK PLAN

DATE: DECEMBER 16, 2019

PRESENTED BY: DENNIS MALONEY, CHAIR

SUMMARY:

Finance Committee Chair, Dennis Maloney, has requested an agenda item to discuss the 2020 Finance Committee work plan. Attached is a preliminary draft of the work plan.
Quarterly Reports: material exceptions will be discussed at monthly FC meetings

- Sales & Use Tax Reports
- Financial Statements
- Capital Improvement Program Reports
- Enterprise Dashboards (recreation, golf, utilities)
- Cash and Investments Reports

Major Initiatives for 2020:

- Biennial Budget Process – Program
  Budgeting utilizing zero-based concepts and processes
- Capital budgeting processes and delivery efficiencies
- Dashboards to Staff Initiative
- KPI Review
- Fee for service methodologies
- Building Fees – comprehensive review and comparison with neighboring cities
- BAPS, TIFS, and other development encouraging tools
- External IT security audit

Third Quarter

- Biennial Budget Process (July, Aug)
- Tap fee review
- Quarterly Reports that are available (July)
- Revenue Projection Dashboards (July)
- Presentation from Eide Bailly on Audit of 2019 CAFR (July)
- Remaining Quarterly Reports (Aug)
- Revenue Projection Dashboards (Aug)
- Financial Policies – possible amendments (Aug)
- Preliminary Assessed Valuation (Sept)

Fourth Quarter

- Quarterly Reports that are Available (Oct)
- Charges for Services & Fees for 2021 (Oct)
- Revenue Projection Dashboards (Oct)
- Review 2021-2022 Biennial Budget (Oct)
- Review Non-Profit Grant applications (Nov)
- Completion of IT security audit

First Quarter

- Biennial Budget Process (Jan, Feb, Mar)
- Quarterly Reports that are available (Jan)
- Write-offs of Accounts Receivable (Feb)
- Remaining Quarterly Reports (Feb)
- Capital budgeting processes and delivery efficiencies (Mar)
- Initial discussion of IT security audit scope

Second Quarter

- Biennial Budget Process (April, June)
- Presentation from Chandler on Economy and Investments (Apr)
- Quarterly Reports that are available (Apr)
- Review Renewal and Replacement schedules for Recreation Center and Golf Course (Apr)
- Recreation Center Fees (Apr)
- Remaining Quarterly Reports (May)
- Budget Amendment (May)
  - 2018 carryover
  - 2019 changes