City of
Coeur d'Alene
IDAHO

A CONTINUED MEETING OF THE CITY COUNCIL
June 2, 2022, 9:00 A.M.
Library Community Room

AGENDA

***All items are deemed action items, in that Council may provide direction to staff regarding budget preparations.**

A. CALL TO ORDER-

1. Overview of 2022-2023 Financial Plan

   Presented by: Troy Tymesen, City Administrator and Vonnie Jensen, Comptroller

2. Updates from Departments with Significant Financial Changes

3. Council priority discussion

4. Next Steps

Presented by: Troy Tymesen, City Administrator

B. ADJOURNMENT

City of Coeur d'Alene
ARPA Fund Requests

				To Be
		Included in	Include in	Included in
		2021-22	2022-23	2023-24
Dept.	Description	Budget ??	Budget ??	Budget ??
Building Dept	Inspection Vehicles		$62,000	
Building Maint.	HVAC Upgrades - Streets & Engineering		47,000	
Building Maint.	Street Dept Flooring / Lighting / Windows		30,000	
Fire	Self Contained Breathing Apparatus		986,610	
Legal	Integrated Case Management System		71,850	8,625
Municipal Services - IT	Network Upgrade Project		547,855	
Municipal Services - IT	Wireless AP Replacement Project	39,175		
Parks	Turf Sweeper		40,000	
Parks	Turf Vehicles		30,000	
Parks	Mower		19,000	
Parks	Spreader		10,000	
Parks	Trailer		30,000	
Parks	Tractor		65,000	
Police	Police Station Expansion		3,000,000	1,600,000
Recreation	Pickup Truck		35,000	
Streets	Western Star Dump Truck with plow and snowgate	247,086		
Streets	Vehicle Replacement		270,000	
Streets	Crack Sealer		92,000	
Streets	Street Shop Remodel		600,000	
		286,261	5,936,315	1,608,625
				7,831,201
Total Funds: $8,659,329				(828,128)
Grant period: 3/3/2021 to 12/31/2024				

MUNICIPAL SERVICES/INFORMATION TECHNOLOGY BUDGET FY 2022-2023

2022 AND BEYOND, IT'S ALL ABOUT SECURITY

HACKERS CONDUCTING SOCIAL ENGINEERING… Why is this important? Because people, not technology, represent the biggest weakness and vulnerability to an organization. To defend our organizations against this, one needs to properly prepare themselves and staff to recognize social engineering methods and how to handle them internally~ TRAINING, TRAINING, TRAINING.

KNOWBE4: training conducted in conjunction with ICRMP.

RANSOMWARE…

VULNERABILITIES: SOLAR WINDS; MICROSOFT EXCHANGE; GOOGLE CHROME; APPLE WEBKIT; DUO ACTIVE DIRECTORY

LARGEST ATTACKS BY INDUSTRY

- **Business Services**: A consulting firm was initially silent about being attacked by a gang that claimed to have lifted 6 terabytes of data from its servers**. The group demanded $50 million in ransom and published some files online to prove its point.**
- **Food and agriculture:** An internationally owned meatpacking conglomerate briefly shuttered plants and stopped deliveries of its products to grocers in June, which resumed **after the company paid $11 million in ransom to an organization the FBI identified as a cybercrime syndicate.**
- **Insurance:** An insurer made **a $40 million ransom payment** to regain control of its systems. This is believed to be the largest ransomware payment to date.
- **Law enforcement:** One of the worst ransomware attacks against police targeted the police department in a major U.S. city. **A cybergang demanded $4 million in ransom and released police disciplinary files.**
- **Tech:** A computer company was hit with **a $50 million extortion attempt**. The cybercriminals posted sensitive documents online to back up their threat, and warned that they'd double the ransom demand if it wasn't paid quickly.

Key trends in the cybersecurity area:

- Governments increased efforts to disrupt and take legal action against state-sponsored threat actors.
- Cybercriminals are increasingly motivated by the monetization of their activities. As a result**, cryptocurrency remains the most common pay-out method for threat actors.**
- The two most common ransomware infection vectors are compromised through **phishing emails and brute-forcing on Remote Desktop Services.**
- Malware targeting container environments have become much more dominant.
- The Phishing-as-a-Service business model is more popular.

Taken from: Shieldoo Blog post

WHAT CAN BE DONE?

Zero Trust=Is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications.

2 Factor Authentication = is a process which requires two steps in order to verify a user. Rather than just asking for a single piece of information – such as a password — two factor authentication goes a step further to enhance the level of security within the system. **If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access: without approval at the second factor, a password alone is useless.**

WHERE ARE WE HEADED?
THERE ARE THREE CATEGORIES OF NEED:

Infrastructure – Legacy Networks with the Castle and Moat Firewall approach are not working. The City's 17 year network needs updates. This will take place over several years due to interruptions to the network, staffing, and funding. Supply chain may also be an issue.

- SAN- Replaced every 5 years
- Physical and Virtual Servers

Resources: Staffing; Currently there are 2 IT Techs to manage day-to-day items; install equipment; update software; manage projects; conduct utility locates; manage approx. 3800 support Tickets and 600 Workstations (upgrades take over 3,000 hours, such as the Windows update every 5 years)

Proposed reorganization of IT, to occur over the next three year. Level 1-3 IT Techs; Application Managers; Arch/Engineer; Division/Department

Security: 2-factor at a minimum, MDM for phone security

FY 22-23

Highlights:

- Personnel increase: Need for another IT Technician **$48,000**
- Software Licensing: The largest expense is moving to Microsoft E3 License, which provides many benefits to security and updates $**373,364**
- City-wide automation: Includes a network upgrade project proposed for ARPA funding **$658,831** (expected to provide a 10 year life cycle)
- Official Representation: Covers the cost of sending flowers to employee for hospital stays/deaths in family. **$500**
- Software/Anti-virus: the cost of existing software has increase an average of 14% **$73,913**
- R/M Security Camera Equipment **$71,244** *(Replacement of all cameras over a 10 year period = 25 per year)*

Infrastructure: Network upgrades, estimate at $547,855 (ARPA Funding sought)

Resources: 1 IT Technician position ($48,000)

Security: ($272,000)
Update to Microsoft E3 Licensing an 2-factor; 2-factor Fobs required

THE BACKBONE OF THE CORPORATION

Without robust security and IT Network the organization leads itself to system outages and malware/ransomware attacks.

Change is hard, but it must occur.

"There is nothing permanent except change." -Heraclitus