City of Valdez

212 Chenega Ave.
Valdez, AK 99686

Meeting Agenda

City Council

Tuesday, March 19, 2024 | **7:00 PM** | **Council Chambers**

Regular Meeting

REGULAR AGENDA - 7:00 PM

I. CALL TO ORDER

II. PLEDGE OF ALLEGIANCE

III. ROLL CALL

IV. APPROVAL OF MINUTES

V. PUBLIC BUSINESS FROM THE FLOOR

VI. CONSENT AGENDA

1. Appointment to the Beautification Commission- Applicant: Donna Lane
2. Appointment to Regional Citizens' Advisory Council Board of Directors - Applicant: Dorothy Moore
3. Proclamation: Earthquake Remembrance Day

VII. NEW BUSINESS

1. Annual Renewal of City/School Health Insurance Benefit Plan for Period Beginning 4/1/2024
2. Approval of Amendment to the 2024 Capital Request for Providence Valdez Medical Center to Fund Various Construction Projects

VIII. ORDINANCES

1. #24-02 - Amending Chapter 10.12 of the Valdez City Code Titled Parking. First Reading. Public Hearing.
2. #24-04 - Amending Chapter 1.08 of the Valdez Municipal Code Titled General Penalty. First Reading. Public Hearing.

3. #24-05 - Amending Chapter 3.24 of the Valdez Municipal Code Titled Public Accommodation Tax. Second Reading. Adoption.

4. #24-06 - Amending Title 6 of the Valdez Municipal Code by Amending Section 6.04.010 Titled Definitions and Section 6.08.020 Titled Running at Large. Second Reading. Adoption.

5. #24-08 - Amending Chapter 6.20 of the Valdez Municipal Code Titled Rabies. Second Reading. Adoption.

IX. RESOLUTIONS

1. #24-08 - Authorizing the Submission of a Local Cybersecurity Grant through the Alaska Division of Homeland Security and Emergency Management to Develop a Cybersecurity Assessment

X. REPORTS

1. Information Technology Department Annual Report

2. Monthly Treasury Report: January 2024

XI. CITY MANAGER / CITY CLERK / CITY ATTORNEY / MAYOR REPORTS

1. City Manager Report

2. City Clerk Report

3. City Attorney Report

4. City Mayor Report

XII. COUNCIL BUSINESS FROM THE FLOOR

XIII. ADJOURNMENT

XIV. APPENDIX

1. Legal Billing Summary - February 2024

File #: 24-0092, **Version:** 1

ITEM TITLE:
Appointment to the Beautification Commission- Applicant: Donna Lane

SUBMITTED BY: Elise Sorum-Birk, Deputy City Clerk

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Review and appoint applicants.

SUMMARY STATEMENT:

The following application has been received to fill the existing vacancy on the Beautification Commission:

- Donna Lane

The term of appointment is for a partial 1.5-year term ending July 31, 2025.

Application materials are attached.

APPLICATION FOR APPOINTMENT TO BOARD OR COMMISSION

BOARD/COMMISSION Beautification Commission

DATE ~~3/6~~ 3/7/24

NAME Donna Lane

RESIDENCE ADDRESS [redacted]

MAILING ADDRESS [redacted]

TELEPHONE NUMBER Daytime [redacted] Evening Same

OCCUPATION retired architect EMPLOYER -

Please check the main reason(s) for applying for appointment to this board/commission:

✓ I have expertise that I want to contribute.
✓ I am interested in the activities the board/commission handles.
___ I want to participate in local government.
___ I am strongly concerned with better government.
___ I want to make sure my segment of the community is represented.
___ Other:_____

Please explain in greater detail those items you have checked: My background/career was in architecture and graphics & talent I can share on the commission. I have served on the commission before

It is suggested you attach an outline of your education, work and volunteer experience.

How did you learn of this vacancy? (circle one)

Media Word of mouth Solicitation Other_____

Donna Lane
Signature

***** Please return this form to the Office of the City Clerk, P.O. Box 307, Valdez, AK 99686 *****

File #: 24-0093, **Version:** 1

ITEM TITLE:
Appointment to Regional Citizens' Advisory Council Board of Directors - Applicant: Dorothy Moore

SUBMITTED BY: Elise Sorum-Birk, Deputy City Clerk

FISCAL NOTES:

Expenditure Required: N/A
Unencumbered Balance: N/A
Funding Source: N/A

RECOMMENDATION:

Appoint Dorothy Moore to serve a two-year term on the Prince William Sound Regional Citizens' Advisory Council

SUMMARY STATEMENT:

The City of Valdez holds two dedicated seats on the PWSRCAC Board of Directors. The dedicated seats for the City represent an opportunity to influence decisions having profound implications for oil transportation safety in Alaska, and for the state's oil spill prevention and response capabilities.

Board members are appointed for a two-year term.

One of the City's two seats will become vacant due to term expiration prior to the May 2024 annual RCAC meeting.

The City Clerk's Office received the attached letter of interest from Dorothy Moore, who has successfully represented Valdez on the board for many years.

Dorothy Moore
[redacted]

March 5, 2024

City of Valdez
P O Box 307,
Valdez, Alaska 99686

Attention Elise Sorum-Birk:

Please forward this letter to the City Council.

Dear Mayor Scheidt and members of the Valdez City Council:

I have called Valdez Home for 75 years and have served as one of Valdez's representatives on the Prince William Sound Regional Citizens Advisory Council since 2007. I would like to serve another two years.

Having lived through the '64 Earthquake and the '89 Oil Spill, I have enjoyed representing Valdez. I find the information stimulating and have the time to devote to the organization.

For the past few years I have participated on the Scientific Committee where I get to listen and learn from PHD's who argue in very large words. (It often reminds me of the playground but with much bigger words). I also sit on the Legislative Affairs committee, and the Board Governance committee

Through these committees and Board in-person meetings, I think I have helped foster a working relationship with the other communities which make up the region of the Exon oil spill. Please consider my request to continue representing Valdez.

Sincerely

Dorothy M Moore

Dorothy M Moore
[redacted]

File #: 24-0094, **Version:** 1

ITEM TITLE:
Proclamation: Earthquake Remembrance Day

SUBMITTED BY: Sheri Pierce, MMC, City Clerk

FISCAL NOTES:

Expenditure Required: Click here to enter text.
Unencumbered Balance: Click here to enter text.
Funding Source: Click here to enter text.

RECOMMENDATION:

Click here to enter text.

SUMMARY STATEMENT:

The attached proclamation respectfully recognizes those citizens who lost their lives in the 1964 Earthquake. The proclamation will be read on March 27th at the Earthquake Remembrance Ceremony which will be held at the Tom Kelsey Dock at 5:30 pm.

PROCLAMATION

WHEREAS, in the early evening hours of Friday, March 27, 1964, the original Valdez townsite, home to about 800 persons was jolted, along with most of southcentral Alaska, by one of the most forceful earthquakes of the century; and

WHEREAS, the earthquake—which lasted 5.5 minutes and measured 9.2 on the Richter scale—triggered submarine landslides causing substantial water disturbance in Port Valdez, inundating the community and destroying the City dock in Valdez, at which the Alaska Steamship Company vessel "Chena" was moored, unloading cargoes; and

WHEREAS, the lives of 31 Valdezeans in the boat harbor or standing on the dock were taken when that structure collapsed and disappeared under the waters of Port Valdez; and

WHEREAS, thereafter, either as a direct or indirect result of this natural disaster, a total of 38 persons lost their lives in Valdez, including the four-member crew of an Alaska Air National Guard airplane; and

WHEREAS, the original Valdez townsite was subsequently condemned as unsuitable for continued use and the remaining residents of Valdez came together with assistance from local, state, and federal public officials to create a new townsite; and

WHEREAS, the people of Chitina, Copper Center, Glennallen, Fairbanks and other Alaska communities responded immediately to the needs of Valdez in the highest tradition of compassion; and

WHEREAS, in the intervening 60 years, the families and friends of those who perished have borne their sorrow quietly and with diminishing public awareness of their personal tragedies.

NOW, THEREFORE, I, Sharon Scheidt, Mayor of the City of Valdez, do hereby proclaim Wednesday, March 27, 2024 as

EARTHQUAKE MEMORIAL REMEMBRANCE DAY

and urge citizens to pause and remember those Valdezeans who lost their lives during the 1964 earthquake.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri Pierce, City Clerk, MMC

File #: 24-0091, **Version:** 1

ITEM TITLE:
Annual Renewal of City/School Health Insurance Benefit Plan for Period Beginning 4/1/2024

SUBMITTED BY: Rhea E Cragun, Human Resource Director

FISCAL NOTES:

Expenditure Required: $4.5MM (City, April-December 2024)
Unencumbered Balance: $4.5MM
Funding Source: Cost code 41300, pro-rated among all staffed departments

RECOMMENDATION:

Approve

SUMMARY STATEMENT:

- This agenda item formalizes the annual renewal of the health insurance benefit plan.
- This health insurance renewal with a 21% increase is estimated to increase the FTE Payroll Budget Category (comprised of Salaries/Wages + Benefits) 3-4% in the 2025 Budget.
- The schools have separately reviewed and approved their plan renewal specifications.
- Renewal Premium Change:
    - City +20.6%: total monthly $2341.89 to $2825.80
        - Employer monthly: $2248.22 to $2712.77
        - Employee monthly: $93.67 to $113.03
    - School: +6.9%
- Plan Changes:
    - Stop loss rates renewed with +15.9% to premium
    - Hearing Exam coverage modified:
        - Prior Coverage: Employee pays 10% exam when device is purchased. Device 50%. Maximum every 3 Years
        - Change: Employee pays 10% exam (regardless of device purchase or not).

Device 50%. Maximum every 3 Years (estimated cost increase +$3000/yr)

City of Valdez
2023 Employee Benefits Plan: **Total Cost**

April 1, 2024 Renewal

		Current Meritain/HCC Projected Costs	Renewal Meritain/HCC Projected Costs
Individual Stop Loss (ISL) Deductible		$175,000	$175,000
Fixed Costs	131	$264.76	$300.88
Consulting Fee	131	$20.28	$20.89
Total Fixed Fees		**$285.04**	**$321.77**
% Change from Current			**12.9%**
Expected Costs			
Medical/Rx	131	$1,910.29	$2,334.63
Dental Claims	131	$117.51	$145.82
Vision Claims	131	$48.02	$44.47
Total Expected Costs		**$2,360.86**	**$2,846.69**
			20.6%
Maximum Costs			
Medical/Rx	131	$2,271.81	$2,716.90
Dental Claims	131	$117.51	$145.82
Vision Claims	131	$48.02	$44.47
Total Maximum Costs		**$2,722.38**	**$3,228.96**
			18.6%
Total Monthly Expected Cost		**$309,273**	**$372,917**
Total Annual Expected Cost		**$3,711,276**	**$4,475,001**
% Change from Current			**20.6%**
Total Monthly Maximum Liability		**$356,632**	**$422,994**
Total Annual Maximum Liability		**$4,279,585**	**$5,075,930**
% Change from Current			**18.6%**

Notes

1. Renewal expected claims based on PS&F projection blending current and prior years.
2. Broker fee based on current fee of $63,760 with a 3% increase per year, shared between City of Valdez and Valdez City Schools.

2024 EMPLOYEE BENEFITS PLAN

CITY OF VALDEZ, ALASKA
OPPORTUNITIES IN EVERY SEASON

PRESENTED ON:
1/31/2024

PRESENTED BY:

COLLEEN SAVOIE	ACCOUNT EXECUTIVE
KEVA PEAIRS	ACCOUNT EXECUTIVE
SHELLY TUTTLE	SR ACCOUNT MANAGER
DAVID MONTGOMERY	ANALYST

PARKER SMITH & FEEK
An IMA Company

PRE-RENEWAL AGENDA

1. PS&F Updates
2. Renewal Updates
3. Timeline & Next Steps

Your PS&F Team

COLLEEN SAVOIE
Account Executive

KEVA PEAIRS
Account Executive

SHELLY TUTTLE
Senior Account Manager

DAVID MONTGOMERY
Senior Account Analyst

2024 Renewal Projection

City of Valdez

Summary Page

	Claims Comparison	Medical/Rx	Dental	Vision	Total
1	2023 Current Claim Liability	$1,910.29	$117.51	$48.02	$2,075.82
2	2024 Renewal Claim Liability	$2,334.63	$145.82	$44.47	$2,524.92
3	% Difference (renewal impact)	**22.2%**	**24.1%**	**-7.4%**	**21.6%**

	Fixed Fees	Medical/Rx	Dental	Vision	Total
4	2023 Current Fixed Fees	$282.04	$2.20	$0.80	$285.04
5	2024 Renewal Fixed Fees	$318.77	$2.20	$0.80	$321.77
6	% Difference (renewal impact)	**13.0%**	**0.0%**	**0.0%**	**12.9%**

	Total Liability Comparison	Medical/Rx	Dental	Vision	Total
7	2023 Current Total Liability	$2,192.33	$119.71	$48.82	$2,360.86
8	2024 Renewal Total Liability	$2,653.40	$148.02	$45.27	$2,846.69
9	% Difference (renewal impact)	**21.0%**	**23.6%**	**-7.3%**	**20.6%**

Notes

1. Please note that these are estimates based on information at a specific point in time and are subject to change.
2. Enrollment has been lagged by 2 months for medical and Rx, by 1 month for dental and vision.

City of Valdez
2024 Employee Benefits Plan: **Summary**

April 1, 2024 Renewal

	Current		Renewal	
Total Benefit Cost	**Carriers**	**Cost**	**Carriers**	**Cost**
Medical	Meritain / HCC	$3,474,602	Meritain / HCC	$4,143,029
PCORI Fee	IRS	$1,233	IRS	$1,233
Dental	Meritain	$184,726	Meritain	$229,229
Vision	Meritain	$75,487	Meritain	$69,907
Life / AD&D	Prudential	$347	Prudential	$409
Consulting Fee	PS&F	$31,880	PS&F	$32,836
Total Annual Premiums / Cost	**$3,768,276**		**$4,476,644**	
$ Change from Current	-		$708,368	
% Change from Current	-		18.8%	

Notes

1. PCORI Fee assumes PMPY fee of $3.22 and member count of 383.

City of Valdez
2023 Employee Benefits Plan: **Total Cost**

April 1, 2024 Renewal

		Current Meritain/HCC Projected Costs	Renewal Meritain/HCC Projected Costs
Individual Stop Loss (ISL) Deductible		$175,000	$175,000
Fixed Costs	131	$264.76	$300.88
Consulting Fee	131	$20.28	$20.89
Total Fixed Fees		**$285.04**	**$321.77**
% Change from Current			**12.9%**
Expected Costs			
Medical/Rx	131	$1,910.29	$2,334.63
Dental Claims	131	$117.51	$145.82
Vision Claims	131	$48.02	$44.47
Total Expected Costs		**$2,360.86**	**$2,846.69**
			20.6%
Maximum Costs			
Medical/Rx	131	$2,271.81	$2,716.90
Dental Claims	131	$117.51	$145.82
Vision Claims	131	$48.02	$44.47
Total Maximum Costs		**$2,722.38**	**$3,228.96**
			18.6%
Total Monthly Expected Cost		**$309,273**	**$372,917**
Total Annual Expected Cost		**$3,711,276**	**$4,475,001**
% Change from Current			**20.6%**
Total Monthly Maximum Liability		**$356,632**	**$422,994**
Total Annual Maximum Liability		**$4,279,585**	**$5,075,930**
% Change from Current			**18.6%**

Notes

1. Renewal expected claims based on PS&F projection blending current and prior years.
2. Broker fee based on current fee of $63,760 with a 3% increase per year, shared between City of Valdez and Valdez City Schools.

City of Valdez
2024 Employee Benefits Plan: **Budget Rates**

April 1, 2024 Renewal

Rates - Med/Rx/Den/Vis	Counts	Current Meritain / HCC $100 Deductible Total Cost	Renewal Meritain / HCC $100 Deductible Total Cost
Employee	33	$1,096.33	$1,302.49
Employee & Spouse	25	$2,269.40	$2,696.15
Employee & Child(ren)	19	$2,126.88	$2,526.83
Employee & Family	54	$3,343.82	$3,972.61
Monthly Estimated Premium	**131**	$313,891	$372,917
Annual PSF Estimated Premium Total		**$3,766,696**	**$4,475,001**
% Change From Current		-	18.8%
Annual $ Change From Current		-	$708,306
PEPM Consulting Fee		$20.28	$20.89
Self-Insured Totals			
Annual Total at Carrier Maximum		$4,279,589	$5,075,930
Annual Total at Carrier Expected		$3,565,332	$4,221,737
% of Maximum		88%	88%
% of Expected		106%	106%

Printed: 1/31/2024 This is only an outline. Actual rates and contract provisions will be determined by specific carrier.

City of Valdez
2024 Employee Benefits Plan: **TPA**

April 1, 2024 Renewal

		Current Meritain	Renewal Meritain
Administration Fees			
Medical/Rx	131	$28.75	$29.15
Aetna Network		15% of savings	15% of savings
The Alaska Preferred Provider Network		25% of savings	25% of savings
Utilization Management	131	$2.55	$2.75
Case Management		$160 / hour	$160 / hour
COBRA Administration	131	$1.40	$2.40
Teladoc	131	$3.10	$3.10
Healthy Merits	131	$4.50	$4.50
PBM Interface Fee	131	$2.00	$2.00
National Cooperative Rx PMPM Fee	383	$0.20	$0.20
Transcarent	131	$2.70	$2.70
NSA Air Ambulance Administration	131	$1.00	$1.00
EAP	131	$1.65	$1.65
Consulting Fee	131	$20.28	$20.89
Estimated Total PEPM	**131**	**$68.51**	**$70.72**
Monthly Administration Costs		**$8,975**	**$9,265**
Annual Fixed Costs		**$107,705**	**$111,177**
% Change From Current		**-**	**3.2%**
Additional Charges			
SBC Preparation		$250 per year	$250 per year
Hinge Health per Participant		$250 Acute, $995 Chronic	$250 Acute, $995 Chronic
Biometric Screening		$190 Onsite, $202 Offsite	$190 Onsite, $202 Offsite
Independent Review		via Medical Rehabilitaion Consultants	via Medical Rehabilitaion Consultants
EAP Provider		Aetna Resources for Living	Aetna Resources for Living
Optional Programs			
Livongo		N/A	$78 PPPM Diabetes Only $80 PPPM Weight Management $80 PPPM Whole Person Health
Notes			
PPO Network - Alaska		Aetna Choice PPO	Aetna Choice PPO
Wrap Network		The Alaska Preferred Provider Network	The Alaska Preferred Provider Network
PBM		Caremark via National Cooperative Rx	Caremark via National Cooperative Rx
Rx Rebates		100% Pass Thru	100% Pass Thru
Additional Notes		Actual network fee costs are not included in totals above.	Actual network fee costs are not included in totals above.

City of Valdez
2024 Employee Benefits Plan: **Stop Loss**

April 1, 2024 Renewal

		Current HCC ISL Level $175,000	Renewal HCC ISL Level $175,000	Option 1 HCC ISL Level $200,000	Option 2 HCC ISL Level $225,000
			Firm through 2/8	Firm through 2/8	Firm through 2/8
Individual Stop Loss Features					
Individual Stop Loss (ISL) Deductible		$175,000	$175,000	**$200,000**	**$225,000**
Annual Maximum		Unlimited	Unlimited	Unlimited	Unlimited
Contract Type		24/12	**Paid**	**Paid**	**Paid**
Benefits covered		Medical, Rx	Medical, Rx	Medical, Rx	Medical, Rx
No New Laser @ Renewal		Included	Included	Included	Included
Rate Cap		50%	50%	50%	50%
ISL Advancement		Included	Included	Included	Included
Experience Refunding		Not Included	Not Included	Not Included	Not Included
Laser(s)		None	None	None	None
Stop Loss Rates					
ISL Premium					
Composite	131	$208.55	$241.78	$216.14	$190.36
Aggregate Premium					
Composite	131	$7.98	$9.27	$9.42	$9.56
Monthly Stop Loss Premiums		$28,365	$32,888	$29,548	$26,190
Total Annual Stop Loss Costs		**$340,385**	**$394,651**	**$354,580**	**$314,274**
% Change From Current		**-**	**15.9%**	**4.2%**	**-7.7%**
$ Change From Current		**-**	**$54,265**	**$14,195**	**-$26,111**
Commissions		Net	Net	Net	Net
Aggregate Stop Loss Factors					
Contract Type		24/12	**Paid**	**Paid**	**Paid**
Aggregate Corridor		125%	125%	125%	125%
Benefits covered		Medical, Rx	Medical, Rx	Medical, Rx	Medical, Rx
Monthly Accommodation		Not Included	Not Included	Not Included	Not Included
Annual Reimbursement Maximum		$1,000,000	$1,000,000	$1,000,000	$1,000,000
Plan Mirroring		Included	Included	Included	Included
Minimum Attachment Point		100%	100%	100%	100%
Aggregate Factors					
Composite	131	$2,271.81	$2,716.90	$2,779.93	$2,841.01
Monthly Aggregate Factors		$297,607	$355,914	$364,171	$372,172
Annual Maximum Claims		**$3,571,285**	**$4,270,967**	**$4,370,050**	**$4,466,068**
% Change From Current		**-**	**19.6%**	**22.4%**	**25.1%**
Annual Expected Claims		$2,857,028	$3,416,773	$3,496,040	$3,572,854
% Change From Current		-	19.6%	22.4%	25.1%
Dental Expected Claims					
Dental Expected Claims	131	$117.51	$145.82	$145.82	$145.82
Monthly Expected Claims		$15,394	$19,102	$19,102	$19,102
Annual Expected Claims		$184,726	$229,229	$229,229	$229,229
Vision Expected Claims					
Vision Expected Claims	131	$48.02	$44.47	$44.47	$44.47
Monthly Expected Claims		$6,291	$5,826	$5,826	$5,826
Annual Expected Claims		$75,487	$69,907	$69,907	$69,907

Printed: 1/31/2024 This is only an outline. Actual rates and contract provisions will be determined by specific carrier.

City of Valdez
2024 Employee Benefits Plan: **Stop Loss**

April 1, 2024 Renewal

	Current HCC ISL Level $175,000	Renewal HCC ISL Level $175,000	Option 1 HCC ISL Level $200,000	Option 2 HCC ISL Level $225,000
		Firm through 2/8	Firm through 2/8	Firm through 2/8
Projected Cost Analysis TPA	Meritain	Meritain	Meritain	Meritain
Annual Fixed Costs				
Total Administration Fees	$107,705	$111,177	$111,177	$111,177
Stop Loss Premiums	$340,385	$394,651	$354,580	$314,274
Total Est. Fixed Costs	**$448,090**	**$505,827**	**$465,757**	**$425,451**
% Change From Current	-	**12.9%**	**3.9%**	**-5.1%**
Total Projected Claims				
Total Maximum Claims	$3,831,498	$4,570,103	$4,669,186	$4,765,204
Total Expected Claims	$3,117,241	$3,715,909	$3,795,176	$3,871,990
Total Liability				
Annual Total at Maximum	**$4,279,589**	**$5,075,930**	**$5,134,943**	**$5,190,654**
% Change From Current	-	**18.6%**	**20.0%**	**21.3%**
$ Change From Current	-	**$796,341**	**$855,354**	**$911,066**
Annual Total at Expected	**$3,565,332**	**$4,221,737**	**$4,260,933**	**$4,297,441**
% Change From Current	-	**18.4%**	**19.5%**	**20.5%**
$ Change From Current	-	**$656,405**	**$695,601**	**$732,109**
Notes				

1. Enrollment counts based on Meritain December enrollment.

City of Valdez
2024 Employee Benefits Plan: **Medical Single Benefits**

April 1, 2024 Renewal

Benefits	Current & Renewal Meritain Grandfathered $100 Deductible	Renewal Meritain Grandfathered Hearing Exam Enhancement
In-Network Member Cost Sharing	**Aetna - Choice POS II**	**Aetna - Choice POS II**
Deductible (Ind. / Fam.)	$100 / $300	$100 / $300
Aggregate (Y/N)	No	No
Out-of-Pocket Maximum (Ind. / Fam.)	$488 per person	$488 per person
Aggregate (Y/N)	No	No
HDHP (HRA/HSA)	No	No
Office Visit - Primary	10%	10%
Specialist	10%	10%
Teladoc	0%*	0%*
Telehealth Visit	10%	10%
Preventive Care Visit	10%	10%
Outpatient Lab & X-Ray	10%	10%
Ambulatory Surgical Center	10%	10%
Transcarent Surgery Benefit	0%*	0%*
Inpatient Hospital	10%	10%
Emergency Room	10%	10%
Urgent Care	10%	10%
Spinal Manipulations	10%	10%
Limitations	40 visits per calendar year	40 visits per calendar year
Outpatient Rehabilitation	10%	10%
Limitations	24 visits per calendar year	24 visits per calendar year
Hearing	Exam: 10% when aid is purchased* Device: 50%* Maximum every 3 years	**Exam: 10% always** **Device: 50%*** **Maximum every 3 years** **(estimated +$3,000/yr)**
Prescription Drugs		
Generic / Brand	$5 / $10*	$5 / $10*
Mail-Order 90-day	$5 / $10*	$5 / $10*
Out-of-Network Benefits	**All Other Providers**	**All Other Providers**
Deductible (Ind. / Fam.)	Shared w/ in-network	Shared w/ in-network
Coinsurance	10% - 25%	10% - 25%
Out-of-Pocket Maximum (Ind. / Fam.)	Shared w/ in-network	Shared w/ in-network
Notes		

1. * indicates deductible waived.

Printed: 1/31/2024 This is only an outline. Actual rates and contract provisions will be determined by specific carrier.

City of Valdez
2024 Employee Benefits Plan: **Dental**

April 1, 2024 Renewal

Benefits	Current & Renewal Meritain $2,500 Max
In-Network Member Cost Sharing	**Passive Network**
Deductible (Ind. / Fam.)	$25 / $75
Annual Maximum per person	$2,500
Class 1: Diagnostic & Preventive	
Exams	0%* 2 visits per year
Cleanings	0%* 2 visits per year
Fluoride Treatment	0%* 2 visits per year up to 19
X-rays	0%*
Class 2: Basic and Restorative	
Fillings, Simple Extractions	10%
Endodontics (Root Canal)	10%
Periodontics (Gum Disease)	10%
Class 3: Major	
Crowns, Bridges, Dentures	50%
Implants	50%
Class 4: Orthodontics	50%
Age Limitation	Up to age 19
Notes	

1. * indicates deductible waived.
2. The annual maximum does not apply to pediatric dental care up to age 19.

City of Valdez
2024 Employee Benefits Plan: **Vision**

April 1, 2024 Renewal

Benefits	Current & Renewal Meritain Vision Plan
In-Network Member Cost Sharing	**Passive Network**
Exam	10%
Lenses	
Single Vision	10%
Bifocal	10%
Trifocal	10%
Frames Allowance	10% coinsurance, benefit paid up to $200
Contact Lenses Allowance	50%
Lasik	$2,000 Lifetime Maximum
Frequency	
Exam	1 per calendar year
Lenses	1 pair per calendar year
Frames	per 2 calendar years
Contact Lenses	1 pair hard lenses or 12 month supply disposable per calendar year
Notes	

1. The annual maximum does not apply to pediatric vision care up to age 19.
2. Both contacts and lenses are covered in same calendar year.

City of Valdez
2023 Employee Benefits Plan: **Basic Life, AD&D**

Basic Life / AD&D	Prudential Current		Prudential Renewal	
FINANCIAL				
Annual Premium	$347		$409	
Rate Guarantee	4/1/2024		4/1/2026	
Basic Life Rate				
Rate Basis	Per $1,000		Per $1,000	
Volume / Rate	270,532	$0.094	270,532	$0.113
Basic AD&D Rate				
Rate Basis	Per $1,000		Per $1,000	
Volume / Rate	270,532	$0.013	270,532	$0.013
Dependent Life				
Rate Basis	Per Unit		Per Unit	
Volume / Rate	0	$0.765	0	$0.765
Broker Commissions	Net		Net	
Contributions	Noncontributory		Noncontributory	
Participation Requirement	100%		100%	
ELIGIBILITY				
Class Description				
Class 1	Executives		Executives	
Class 2	Valdez City School District Ees other than Executives		Valdez City School District Ees other than Executives	
Eligibility Hours	30		30	
SCHEDULE OF BENEFITS				
Benefit Schedule	Flat benefit		Flat benefit	
Benefit Maximum				
Class 1	$4,000 ($10,000 AD&D)		$4,000 ($10,000 AD&D)	
Class 2	$2,000 ($5,000 AD&D)		$2,000 ($5,000 AD&D)	
Dependent Life	Spouse/DP: $2,500	Child(ren): $1,000	Spouse/DP: $2,500	Child(ren): $1,000
Guarantee Issue	Full Amount		Full Amount	
Age Reductions	To 65% at 65, to 50% at 70		To 65% at 65, to 50% at 70	
PROVISIONS				
Earnings Definition	W2		W2	
Accelerated Death				
Class 1	90% to $124,000		90% to $124,000	
Class 2	90% to $122,000		90% to $122,000	
Conversion	Included; EOI is not required		Included; EOI is not required	
Portability	Not included		Not included	
Waiver of Premium - EP	9 mo		9 mo	
NOTES				

1.Volume based on Prudential December invoice.

Voluntary Life / AD&D	Prudential Current / Renewal	
ELIGIBILITY		
Class Description		
Class 1	Executives	
Class 2	City of Valdez Ees other than Executives	
Eligibility Hours	30	
SCHEDULE - EMPLOYEE		
	Vol Life	Vol AD&D
Benefit Schedule	1 x salary	Amount equal to life amount
Benefit Maximum	$120,000	
Guarantee Issue	Full amount	
Age Reductions	To 65% at 65, to 50% at 70	
SCHEDULE - SPOUSE		
	Vol Life	Vol AD&D
Spouse Benefit Schedule	50% of employee amount	50% of employee amount (40% with child)
Spouse Benefit Maximum	$30,000	
Spouse Guarantee Issue	$25,000	
Spouse Reductions	To 65% at 65, to 50% at 70	
Spouse Maximum % of Employee Coverage	50%	
SCHEDULE - CHILD		
	Vol Life	Vol AD&D
Child Benefit Schedule	Flat benefit	15% of employee amount (10% with spouse)
	Vol Life	Vol AD&D
Child Benefit Maximum	$10,000	$9,000
	Vol Life	Vol AD&D
Child Benefit - Birth to 2 weeks	Not covered	Full benefit
Child Benefit - 2 weeks to 6 months	Full benefit	
Student Extension Age	25	
Child Maximum % of Employee Coverage	50%	
PROVISIONS		
Earnings Definition	W2	
Accelerated Death		
Class 1	90% to $124,000	
Class 2	90% to $122,000	
Conversion	Included; EOI is not required	
Portability	Not included	
Waiver of Premium - EP	9 mo	

Printed: 1/31/2024 This is only an outline. Actual rates and contract provisions will be determined by specific carrier.

City of Valdez
2023 Employee Benefits Plan: **Vol Life, AD&D Rates**

Voluntary Life / AD&D	Prudential Current / Renewal	
FINANCIAL		
Rate Guarantee	4/1/2026	
Employee Voluntary Life Rate		
Rate Basis	Per $1,000	
	0 - 19	$0.068
	20 - 24	$0.068
	25 - 29	$0.068
	30 - 34	$0.085
	35 - 39	$0.102
	40 - 44	$0.179
	45 - 49	$0.264
	50 - 54	$0.468
	55 - 59	$0.748
	60 - 64	$1.139
	65 - 69	$1.938
	70 - 74	$3.264
	75 - 79	$5.211
	80+	$5.211
Spouse Voluntary Life Rate		
Rate Basis	Per $1,000	
	0 - 19	$0.068
	20 - 24	$0.068
	25 - 29	$0.068
	30 - 34	$0.085
	35 - 39	$0.102
	40 - 44	$0.179
	45 - 49	$0.264
	50 - 54	$0.468
	55 - 59	$0.748
	60 - 64	$1.139
	65 - 69	$1.938
	70 - 74	$3.264
	75 - 79	$5.211
	80+	$5.211
Child Voluntary Life Rate		
Rate Basis	Per $1,000	
Rate	$0.101	
Employee Voluntary AD&D Rate	Employee	Family
Rate Basis	Per $1,000	
Rate	$0.014	$0.034
Broker Commissions	Net	
Participation Requirement	20%	

2024 Renewal Projection

City of Valdez

Calculation Page

	Claim History and Projection	Medical	Rx	Dental	Vision	Total
	Current Rolling 12 Months					
1	Paid Claims (01/23 to 12/23)	$3,124,763	$709,871	$234,373	$55,879	$4,124,886
2	- Pooled Claimants (>$175,000)	($268,046)	n/a	n/a	n/a	($268,046)
3	x Benefit Adjustment	0.0%	0.0%	0.0%	21.8%	0.3%
4	/ Number of Employees (Lagged)	1,578	1,578	1,578	1,578	1,578
5	= Net Paid Claims PEPM	$1,810.34	$449.85	$148.53	$43.13	$2,451.85
6	Trend % Utilized (Group Specific)	8.4%	11.4%	4.0%	3.0%	
7	x Applied Trend (15 months)	1.106	1.144	1.050	1.038	
8	+ Non-Pooled Claimant Dollars	$110.90	n/a	n/a	n/a	$110.90
9	Rx Rebates	$0.00	($116.98)	$0.00	$0.00	($116.98)
10	= Projected Paid Claims	$2,113.28	$397.87	$155.99	$44.75	$2,711.89
11	Period Weighting	70.0%	70.0%	70.0%	70.0%	70.0%
	Prior Rolling 12 Months					
12	Paid Claims (01/22 to 12/22)	$2,194,791	$662,279	$170,221	$51,262	$3,078,553
13	- Pooled Claimants (>$175,000)	($627,703)	n/a	n/a	n/a	($627,703)
14	x Benefit Adjustment	0.0%	0.0%	0.0%	21.8%	0.5%
15	/ Number of Employees (Lagged)	1,521	1,521	1,523	1,523	1,521
16	= Net Paid Claims PEPM	$1,030.30	$435.42	$111.77	$40.99	$1,618.68
17	Trend % Utilized (Group Specific)	8.4%	11.4%	4.0%	3.0%	
18	x Applied Trend (27 months)	1.199	1.275	1.092	1.069	
19	+ Non-Pooled Claimant Dollars	$230.11	n/a	n/a	n/a	$230.11
20	Rx Rebates	$0.00	($97.85)	$0.00	$0.00	($97.85)
21	= Projected Paid Claims	$1,465.43	$457.29	$122.08	$43.81	$2,088.61
22	Period Weighting	30.0%	30.0%	30.0%	30.0%	30.0%
23	Blended Projected Paid Claims	**$1,918.93**	**$415.70**	**$145.82**	**$44.47**	**$2,524.92**

Notes

1. Please note that these are estimates based on information at a specific point in time and are subject to change.
2. Enrollment has been lagged by 2 months for medical and Rx, by 1 month for dental and vision.

DISCLOSURE OF COMPENSATION

This document constitutes Parker, Smith & Feek's compensation disclosure to City of Valdez ("Client") for purposes of Section 408(b)(2) (codified at 29 U.S.C. § 1108(b)(2)(B)) of the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), which provides an exemption under the prohibited transaction rules with respect to group health plans that enter "reasonable" contracts or arrangements with a covered service provider for the provision of brokerage or consulting services (as detailed in Schedule A below). Such disclosure is generally required where, in connection with furnishing services to the plan, a broker or consultant (or an affiliate or subcontractor thereof) reasonably expects to receive $1,000 or more (as adjusted) in compensation, whether direct or indirect, during the applicable term.

The descriptions of compensation provided below are intended to be prospective in nature, may include reasonable estimates and be described in general terms, and may prove to be unreflective of the actual compensation received by Parker, Smith & Feek during the applicable contract period. Further, this disclosure is limited to Parker, Smith & Feek's compensation for those services associated with Client's group health plan(s) and is not a statement, invoice, or summary of all compensation to which Parker, Smith & Feek may be entitled.

Further, Parker, Smith & Feek will disclose any change to this information to the responsible plan fiduciary, as soon as practicable, but in no event later than sixty (60) days from the date on which Parker, Smith & Feek is informed of such change (unless such disclosure is precluded due to extraordinary circumstances beyond Parker, Smith & Feek's control, in which case the information will be disclosed as soon as practicable).

If you have questions or concerns about anything included in this disclosure, please notify your Parker, Smith & Feek Benefits team. We appreciate your business and continue to be committed to serving your employee benefits needs.

Schedule A

Brokerage and Consulting Services

Strategic Plan Consulting

Technical Plan Consulting

Day-to-Day Administrative Issues

Employee Communications

Schedule B

Expected Compensation for Group Health Plans

Direct and Indirect Compensation

The following describes the direct and indirect compensation that Parker, Smith & Feek (or an affiliate or subcontractor thereof) reasonably expects to receive for the brokerage and consulting services set forth above. Direct compensation includes compensation received directly from the covered plan(s), including arrangements where a plan vendor coordinates the collection and payment of a prearranged fee on Parker, Smith & Feek's behalf, in connection with the provision of brokerage or consulting services to the plan(s) during the applicable contract period. Indirect compensation includes compensation that Parker, Smith & Feek reasonably expects to receive from sources other than the group health plan(s) or plan sponsor, such as standard commissions or fees. Additional forms of indirect compensation are set forth separately below.

Benefit	Payer	Expected Compensation
Consulting Fees	City of Valdez	$31,880

Non-Cash Compensation

Parker, Smith & Feek and its representatives may receive certain non-monetary compensation from insurance companies or other plan vendors that are not made in connection with a particular client or plan. Such compensation may include gifts valued at less than $100 annually, occasional meals and entertainment, or reimbursements in connection with educational meetings, workshops or events, or marketing or advertising initiatives, including services for identifying prospective clients. Plan vendors or service providers may also pay , or reimburse Parker, Smith & Feek for the costs associated with education or training events that may be attended by Parker, Smith & Feek and its representatives, or for Parker, Smith & Feek - sponsored conferences and events. This non-cash compensation may not be solely related or allocable to any particular client or plan.

City of Valdez
2024 Employee Benefits Plan:
Disclosures & Assumptions

A.M. Best Rating – **Parker, Smith & Feek** has a Security Committee which reviews the financial condition of the carriers represented in our proposals. In view of the ever changing healthcare insurance marketplace, and the increasing frequency of insurance company ownership changes and financial stability of these insurance companies, Parker, Smith & Feek's Security Committee has established as a minimum standard, the use of insurance companies rated "A-" Class VII ($50 million to $100 million policy holder surplus) or better by A. M. Best Company. We believe that higher standards are always in the best interest of our clients.

Within this proposal, we have shared the present A.M. Best financial ratings of the insurance carriers being presented. By acknowledgement of this proposal, you have been made aware of the A.M. Best rating of your insurance company for your insurance coverages. By your decision(s) of insurance company, you understand that Parker, Smith & Feek is not responsible for the financial integrity of your insurance company selection and that any issues arising from the financial failure of your insurance company is not Parker, Smith & Feek's liability.

A signed acknowledgement form is required before the initial date of coverage.

Carriers	A.M Best Rating	Carriers	A.M Best Rating
Aetna	A (XV)	OBI (Oregon Business & Industry)	N/A
AFLAC	A+ (XV)	OBI Health Net Plan of Oregon, INC	NR
American Fidelity Assurance Company	A+ (X)	OBI Samaritan Health Plans	NR
Ameritas	A (XV)	PacificSource Health Plans	A- (IX)
CIGNA	A (XV)	Pan-America Life Insurance Company	A (IX)
Colonial Life	A (XV)	Physicians Insurance	A- (IX)
Commencement Bay	A (XV)	Premera Blue Cross	A (XIII)
Companion	A+ (XV)	Principal Life Insurance Company	A+ (XV)
Delta Dental of WA	NR	Providence Health Plan	NR
Everest Re	A+ (XV)	Prudential Insurance Company of America	A+ (XV)
Eye Med Vision Care HMO	NR	QBE A&H	A (XV)
Guardian Life Insurance Company of America	A++ (XV)	Regence Blue Cross Blue Shield	A (XV)
Hartford Life Insurance Company	A+ (XV)	Regence Blue Shield	A (XV)
HCC Life Insurance Company	A++ (X)	Reliance Standard	A++ (XIV)
Health Net (Direct)	NR	Standard	A (XIV)
HM Life Insurance Company	A (XV)	Sun Life	A+ (XV)
HMSA	NR	Symetra	A (XV)
Kaiser	NR	Trustmark	A- (IX)
Kaiser Foundation Health Plan of NW	NR	UHA	NR
Kaiser Foundation Health Plan of WA (GHC)	NR	Unimerica (Optum Stoploss)	A (XV)
Kaiser Foundation Health Plan of WA (GHO)	NR	United Healthcare of Oregon INC	A (XV)
Liberty Mutual	A (XV)	United Healthcare	A (XV)
LifeMap	A- (VII)	Unum	A (XV)
LifeWise	A (XIII)	USAble Life	A (IX)
Lincoln	A+ (XV)	Voya (ING)	NR
MetLife	A+ (XV)	VSP	A- (XIV)
Moda Health	B++ (VIII)	Willamette Dental Insurance INC	NR
Mutual of Omaha	A+ (XV)	Willamette Dental of Washington INC	NR
National Guardian Life Insurance Company	A- (VII)	Zurich	A+ (XV)
New York Life Insurance Company	A++ (XV)		

This summary does not constitute a contract. Refer to contracts/booklets for detailed information. In the event of discrepancies with the the contract, the provisions of the contract will take precedence.

HEALTHCARE REFORM MANDATES ARE INCLUDED WHERE GUIDANCE HAS BEEN RELEASED AND INTERPRETED.

General Assumptions

1. 4/1/2024 is the proposed effective date for the plans illustrated.
2. Rates are guaranteed for 12 months (unless otherwise noted) at which time the benefit plans would renew.
3. Insurance companies reserve the right to change their rates with a 30-day advance notice to the insurance broker and/or the employer.
4. The attached information and rates do not constitute a contract. The rates provided are based upon the data provided by City of Valdez. The insurance company reserves the right to change the rates if the final enrolled census is different from the census data provided. Final rates will be determined by actual enrollment and completed risk questionnaire (if applicable).
5. Plan assumes common eligibility.
6. This is a brief summary of benefits and coverages for comparison purposes only and does not constitute a contract. For more details about the coverage, including any exclusions or limitation, please refer to the carrier summaries. For in-force coverage, please refer to your policy and plan booklet.

Employee Eligibility

1. Employer contribution for employee benefit plans are 100% for employees and 100% for dependents. If contribution level is different than what is illustrated, rates may be subject to change.
2. Employees not enrolled in the employer-sponsored plan must have signed waivers of coverage on file.
3. Group Size: Quote based upon 131 employees and 98 dependent units enrolled on the plan.
4. Eligibility: Employees working a minimum of 20 hours per week after a 30 day probationary period.

Medical Assumptions

1. Specialty drugs may be limited to in-network benefits only and only at special pharmacies.
2. Extra-territorial mandates may apply.
3. Healthcare reform mandates included where guidance has been released and interpreted.

Dental Assumptions

1. Late entrant penalties may apply for services other then Preventive and Diagnostic, if an employee or dependent does not enroll within 31 days of becoming eligible. Late entrant penalties do not apply when there is a qualifying event. Refer to carrier Summary of Benefits for details.

City of Valdez
2024 Employee Benefits Plan:
Disclosures & Assumptions

LIFE and AD&D

1. Coverage is available up to the non-medical maximum until evidence of insurability is approved by the insurance company.
2. Please contact Parker, Smith & Feek to request a revised quote if any census information or if any health conditions of any of the proposed participants change.

NETWORK ASSUMPTIONS	IN-NETWORK PROVIDERS	OUT-OF-NETWORK PROVIDERS
Aetna	Paid according to contract	Based on Medicare reimbursement rates. Balance billing may apply.

The above assumptions are a representative list used for this proposal. Specific assumptions vary from one insurance company to another. A complete list of assumptions will be provided to City of Valdez before coverage is placed with the selected insurance company.

BENEFIT SERVICES

PARKER, SMITH & FEEK, INC. OFFERS A VARIETY OF BENEFIT SERVICES. THE FOLLOWING IS ONLY A REPRESENTATIVE LISTING.

We assist our clients with group benefit products, such as:

- Medical and Prescription Drug
- Vision Care
- Dental
- Group Life Insurance
- Accidental Death and Dismemberment
- Long-term and Short-term Disability
- Long-term Care Coverage
- Employee Assistance Programs
- Travel Accident
- Voluntary Benefits

We have additional resources available to assist in the following areas:

- Claims Analysis (when data is available)
- Employee Claims Advocacy
- Benefits Compliance
- Employee Education and Communications
- Total Compensation Statements
- Benefits/Human Resources Website
- Design and Implementation of Wellness Programs
- Integrated Absence Management

We can assist in locating a strong partner for many other administrative services, including, but not limited to:

- COBRA Administration
- Section 125/Flexible Spending Account
- Administration
- Retirement Plan Administration
- Third Party Health Plan Administration
- Actuarial Valuations
- Retirement Plans - Pension, Profit Sharing, 401k/403b

OTHER PS&F SERVICES

In addition to our full range of benefit services, PS&F also offers:

- Business Succession and Estate Planning
- Workers' Compensation Services
- Personal Insurance for Individuals and Families
- Commercial Risk Management Solutions including insurance protection
- Surety Bonds

If you are interested in any additional services, please contact a member of your PS&F Benefits team at 425.709.3600.

File #: 24-0098, **Version:** 1

ITEM TITLE:
Approval of Amendment to the 2024 Capital Request for Providence Valdez Medical Center to Fund Various Construction Projects

SUBMITTED BY: Nathan Duval, Assistant City Manager / Capital Facilities Director

FISCAL NOTES:

Expenditure Required: Click here to enter text.
Unencumbered Balance: Click here to enter text.
Funding Source: Hospital Excess Revenue Fund

RECOMMENDATION:

Approve amendment to the 2024 Capital Request for Providence Valdez Medical Center to fund various construction projects.

SUMMARY STATEMENT:

Multiple projects managed by Providence Valdez Medical Center have progressed in design and are ready for construction. Bids have been received and this amendment to the 2024 budget will fund said projects. The significant 2024 projects include appropriating $1,864,038 for the CT replacement, recognizing an additional $895,336 to the Sterile Processing (SPD) project. Funds come from the excess revenue fund as well as repurposing unspent budget from completed projects.

The attached list for approval encompasses the current suite of Providence managed capital projects and their corresponding budget. Most of the listed projects have been approved with past Council action and their budgets have been updated to reflect current actual and expected expenditures.

No additional 2024 approvals are anticipated. 2025 projects will be prioritized with City projects later this year.

An outline of the available excess revenue funds will be presented to the Council accounting for the contractually obligated “days cash” and other funding obligations i.e. physicians’ recruitment & retention program, and revenue stabilization needs.

#	Project Name	Justification	2023 Appropriation Total	2024 Updated Budget Appropriation Total	Variance from 2023	Notes	Comments
	Sterile Processing Equipment/Room Upgrades	Past end of usable life	$1,000,000	$1,895,336	$895,336	Actual Construction Bid total	100% design complete / Prov Managed. Updated total budget to include equipment, constructions costs and added contingency.
	LTC- 4 Bed Expansion (includes LTC Kitchen Project)	Community health assessment need identified via survey and signifant space constraints for current census	$500,000	$500,000			35% Design request / Prov Managed
	Emergency Department Redesign (includes ER Door Upgrade and Entrance Redesign Projects)	Infection Prevention, security, triage	$2,750,000	$2,750,000			100% design complete / Prov Managed
	CT Replacement	End of usable life	$250,000	$1,864,038	$1,614,038	Actual Construction Bid total	Initial Design Request / Prov Managed. Updated total budget to include equipment, constructions costs and added contingency.
	Facility-wide cameras	End of usable life and inadequate coverage	$100,000	$100,000			100% design complete / Prov Managed
	Air Handler 3 Replacement	Obsolete	$100,000	$100,000			100% design complete / Prov Managed
	Grease Trap Upgrade	Regular back-ups requiring pumping	$75,000	$75,000			Initial Design Request
	Gas appliances in Dietary	More efficient with gas appliances, Current ovens not working well	$0	$0			
	Automation Up-grade		$350,000	$350,000			100% design complete / Prov Managed

		2023	2024	Variance
Priority Level 1	Total Priority 1	$4,250,000	$5,145,336	
Priority Level 2	Total Priority 2	$875,000	$2,489,038	
	Grand Total (All priorities)	$5,125,000	$7,634,373	$2,509,373

Providence

PVMC 2024 Budget

City of Valdez

KEY STATISTICS:

	2021 Actual	2022 Actual	2023 Annualized	2023 Budget	2024 Budget
FTE	**101**	**93**	**103**	**104**	**104**
LTC Patient Days	3550	3562	3576	3340	3477
Patient Days	890	839	585	913	784
ER Visits	1348	1572	1579	1501	1505
Counseling Visits	2297	1807	1924	2595	2617

FINANCIALS - HOSPITAL:

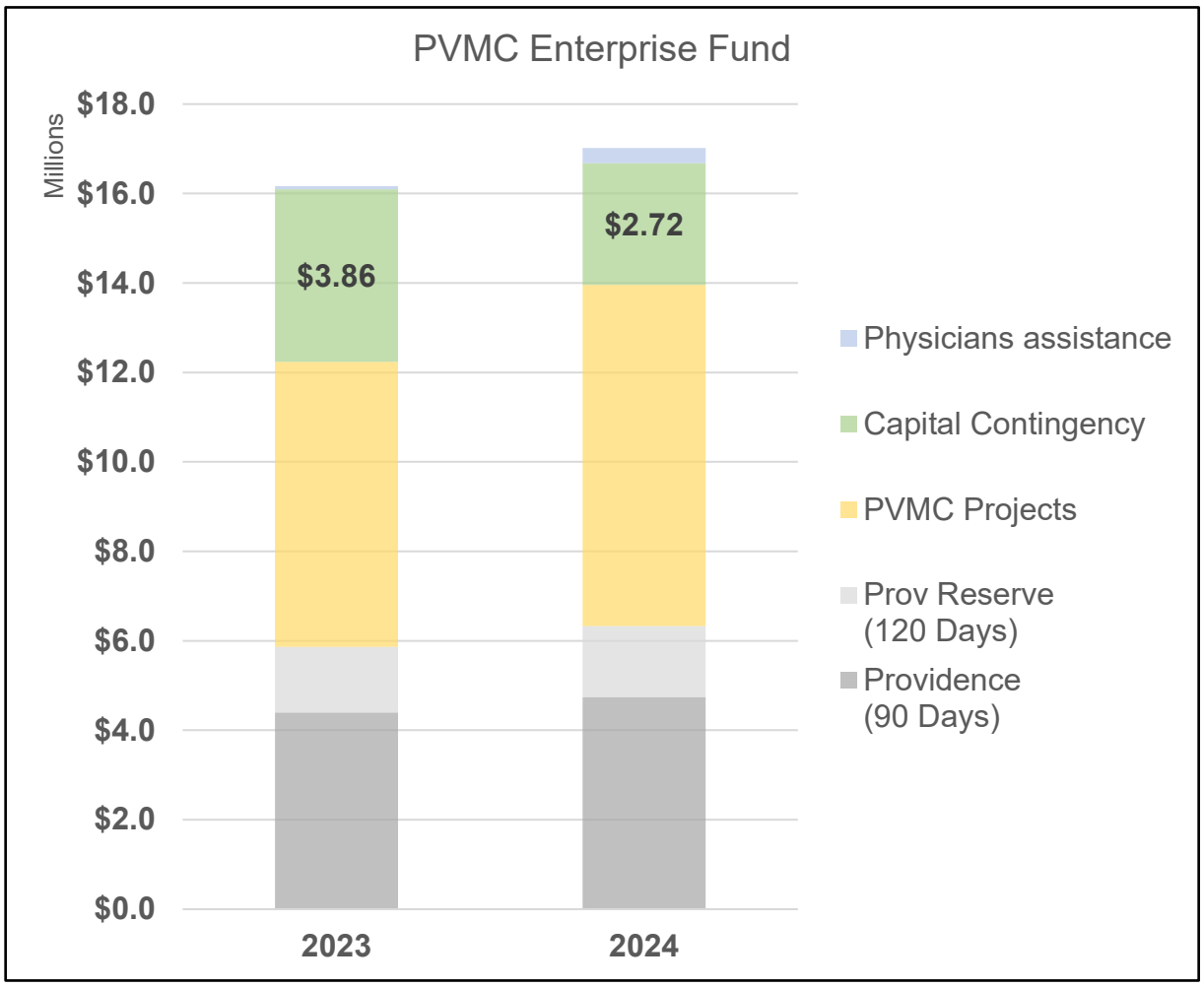
	ACTUAL 2022	BUDGET 2023	Jun-22 12 MTHS TRAILING	BUDGET 2024
Gross Revenue				
LTC/Swing Bed	7,225	6,826	7,278	7,597
Inpatient	3,852	4,502	3,287	3,267
Outpatient	13,165	13,966	13,808	15,613
Primary Care	1,187	1,100	1,354	3,643
Total Gross Revenue	25,429	26,395	25,727	30,120
Net Service Revenue	20,045	22,325	19,314	22,580
Reimb %	78.8%	84.6%	75.1%	75.0%
Other Operating Revenue	416	211	495	237
Net Operating Revenue	20,461	22,536	19,809	22,817
Operating Expenses				
Salaries & Wages	9,988	10,603	10,232	11,586
Employee Benefits	2,307	2,440	2,388	3,008
Professional Fees	847	1,260	755	158
Supplies	1,574	1,632	1,619	1,734
Purchased Services	2,432	2,770	2,504	2,853
All Other Expenses	1,215	718	1,353	1,239
Total Operating Expenses	18,363	19,422	18,851	20,578
EBIDA	**2,627**	**3,114**	**1,493**	**2,789**
% Margin	**12.8%**	**13.8%**	**7.5%**	**12.2%**

FINANCIALS - COUNSELING CENTER:

				Jun-22	
	ACTUAL 2022	BUDGET 2023		12 MTHS TRAILING	BUDGET 2023
Total Gross Revenue	526	838		516	861
Net Service Revenue	264	419		257	431
Reimb %	49.9%	49.9%		49.8%	50.1%
Other Operating Revenue	366	340		360	340
Net Operating Revenue	630	759		617	771
Operating Expenses					
Salaries & Wages	656	744		642	705
Employee Benefits	276	279		303	285
Supplies	9	10		12	12
Purchased Services	68	85		43	49
All Other Expenses	53	37		42	31
Total Operating Expenses	1,062	1,154		1,042	1,082
EBIDA	**-430**	**-395**		**-422**	**-310**
% Margin	-68.3%	-52.1%		-68.4%	-40.2%

CAPITAL EQUIPMENT REQUEST:

Item	Budget
EKG Machines (2)	50,000
Philips Cardiac Monitors (9)	234,000
Postpartum Hemmorrhage Cart	12,000
Dietary Commercial Range	29,000
Ncare for FEES equipment	30,000
Lucas Chest Compression Machine	22,000
Lab iStat	16,000
Lab Blood Bank/Chemistry Refrigerator	15,000
Bed Replacement - Lifecycle replacement	50,000
	$ 458,000



** Physicians Assistance is shown as the remaining portion of a five year contract*
*** 1 Day operating costs 2023= $48,875*
**** 1 Day operating costs 2024 = $52,726*

File #: ORD 24-0002, **Version:** 1

ITEM TITLE:
#24-02 - Amending Chapter 10.12 of the Valdez City Code Titled Parking. First Reading. Public Hearing.

SUBMITTED BY: Sheri Pierce, City Clerk/Bart Hinkle, Police Chief

FISCAL NOTES:

Expenditure Required: N/A
Unencumbered Balance: N/A
Funding Source: N/A

RECOMMENDATION:

Approve Ordinance 24-02 in first reading for public hearing.

SUMMARY STATEMENT:

Current fines and penalties for parking violations have not been updated for a number of years. The existing language relies heavily on the monetary punishment of the impound as a deterrent. The proposed language is designed to have the citation be the primary deterrent method / means of behavior modification by increasing the cost of the citation related to impeding snow removal. Chief Hinkle will be present to discuss operational considerations leading to the proposed language and ordinance change recommended by staff.

Summary of previous action on Ordinance 24-02:

2/6/24: Initial first reading.

2/20/24: During second reading - drafting error was noted - Was postponed to next regular meeting.

3/5/24: Amended to fix drafting error, returned to first reading.

Note:

Ordinance 24-04, the ordinance that runs parallel to this that updates the fine schedule, was amended to change the fine amount from $200 to $80 for impeding snow removal.

Fine amounts in Ordinance 24-02 and Ordinance 24-04 need to match.

CITY OF VALDEZ

ORDINANCE NO. 24–02

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA AMENDING CHAPTER 10.12 OF THE VALDEZ CITY CODE TITLED PARKING

BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, that:

Section 1. Chapter 10.12, Section 10.12.040 (D) of the Valdez Municipal Code is hereby amended to read as follows:

Chapter 10.12

PARKING

Sections:

10.12.010 Parking prohibited on certain streets during certain hours when school in session.
10.12.020 Parking prohibited.
10.12.025 Seasonal parking.
10.12.030 Temporary prohibitions.
10.12.040 Penalty and impoundment.

10.12.010 Parking prohibited on certain streets during certain hours when school in session.

The cul-de-sac area on East Lowe Street extending from the east property line of Lot 1, Block 12, to the east property line of Lot 9, Block 10, is declared to be a no-parking zone for all vehicles except school buses between the hours of seven a.m. and five p.m. on any day when school is in session. (Prior code § 15-8)

10.12.020 Parking prohibited.

No person may park or cause a motor vehicle to be parked, and no motor vehicle may be parked, as follows:

A. On any of the following streets or highways:

1. Meals Avenue from Fidalgo to Robe River Drive, except for the wider parking location on the east side of the street directly in front of the Alaska State Court House,

2. Hazelet Avenue from City Dock to Hanagita,

3. On the north side of Pioneer Drive from Meals Avenue to Tatitlek Avenue;

B. On any street, highway, public way or city-owned parking lot for a period of time longer than twenty-four hours, without special permission of the chief of police;

C. In a private area which is adjacent to a commercial establishment, owned or controlled by another person, in violation of any limitations on parking which have been set, if the area is signed or posted in a manner setting forth the limitations;

D. In a private area which is not adjacent to a commercial area, owned or controlled by another person, without the express permission of that person;

E. At any place or in any position on public or private property, which would block the way of ingress or egress of a motor vehicle to a private area owned or controlled by another person, or which would prevent another from moving a motor vehicle;

F. In any other area where parking has been permanently or temporarily restricted by the city;

G. Any place where the curb has been painted red designates a no parking area. (Ord. 99-07 §§ 1, 2; prior code § 15-9)

10.12.025 Seasonal parking
.
The hourly parking along North Harbor Drive shall be effective from May 1st through September 30th each year. (Ord. 99-07 § 3)

10.12.030 Temporary prohibitions.

A. Notwithstanding any other provision of this title, no person may park or cause a motor vehicle to be parked, and no motor vehicle may be parked, on any street in the city upon which snow removal is undertaken by or on behalf of the city from the time that snow removal operations on the street appear to be necessary until the time that the snow removal operations on the street are completed.

B. The chief of police, or other persons designated by the city manager, is authorized to determine and designate by proper signs, places in which the stopping, standing or parking of a motor vehicle is restricted or prohibited because of traffic conditions, construction, accidents, parades, special events or other purposes deemed by the city to warrant temporary prohibitions on parking, stopping or standing. No person may park, stop or stand a motor vehicle, and no motor vehicle may be parked or stopped, in any area so designated.

C. No person may fail or refuse to immediately move his vehicle when requested to do so by a city police officer or any city employee or contractor engaged in any activity which would be hindered or obstructed in any manner if the vehicle were to remain in the place it occupied at the time the request was made. Upon request, the owner or operator of the vehicle shall move it to a location which does not interfere with the activity which was being hindered or obstructed.

D. Failure to move the vehicle upon request is a separate offense from allowing that vehicle to be parked or stopped in a prohibited area. It is not necessary that a request be made to move the vehicle before the sanctions set forth in Section 10.12.040 may be imposed. (Prior code § 15-10)

10.12.040 Penalty and impoundment.

A. Any vehicle in violation of Section 10.12.020 or 10.12.030 may be impounded by the city, or issued a traffic citation, or both.

B. A vehicle will be impounded from private property only upon the written request of the person who owns or controls the property. Before the vehicle is impounded, the city may require the person requesting the impoundment to sign a statement of ownership or control of the private property involved, and an agreement holding the city harmless for any injury, loss or damage arising from the impoundment.

C. If the vehicle is impounded from either public or private property, this impoundment is done without liability on the part of the city for any damage which may be done to it or its contents. The vehicle shall not be returned to the owner or operator thereof until any impound fees, and any storage or other charges which may have accrued, have been paid.

D. If the vehicle is cited, the penalty for the violation of this ordinance is two-hundred ~~twenty~~ dollars.

E. If the vehicle is both impounded and cited, all impound and citation fees, and other charges, must be paid prior to the return of the vehicle to the owner or operator. (Prior code § 15-11)

Section 2. This ordinance shall take effect immediately upon adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this _____day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstain:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Walker, P.C

CITY OF VALDEZ

ORDINANCE NO. 24–02

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA AMENDING CHAPTER 10.12 OF THE VALDEZ MUNICIPAL CODE TITLED PARKING

BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, that:

Section 1. Chapter 10.12, Section 10.12.040 (D) of the Valdez Municipal Code is hereby amended to read as follows:

Chapter 10.12

PARKING

Sections:

10.12.010 Parking prohibited on certain streets during certain hours when school in session.
10.12.020 Parking prohibited.
10.12.025 Seasonal parking.
10.12.030 Temporary prohibitions.
10.12.040 Penalty and impoundment.

10.12.010 Parking prohibited on certain streets during certain hours when school in session.

The cul-de-sac area on East Lowe Street extending from the east property line of Lot 1, Block 12, to the east property line of Lot 9, Block 10, is declared to be a no-parking zone for all vehicles except school buses between the hours of seven a.m. and five p.m. on any day when school is in session. (Prior code § 15-8)

10.12.020 Parking prohibited.

No person may park or cause a motor vehicle to be parked, and no motor vehicle may be parked, as follows:

A. On any of the following streets or highways:

1. Meals Avenue from Fidalgo to Robe River Drive, except for the wider parking location on the east side of the street directly in front of the Alaska State Court House,

2. Hazelet Avenue from City Dock to Hanagita,

3. On the north side of Pioneer Drive from Meals Avenue to Tatitlek Avenue;

B. On any street, highway, public way or city-owned parking lot for a period of time longer than twenty-four hours, without special permission of the chief of police;

C. In a private area which is adjacent to a commercial establishment, owned or controlled by another person, in violation of any limitations on parking which have been set, if the area is signed or posted in a manner setting forth the limitations;

D. In a private area which is not adjacent to a commercial area, owned or controlled by another person, without the express permission of that person;

E. At any place or in any position on public or private property, which would block the way of ingress or egress of a motor vehicle to a private area owned or controlled by another person, or which would prevent another from moving a motor vehicle;

F. In any other area where parking has been permanently or temporarily restricted by the city;

G. Any place where the curb has been painted red designates a no parking area. (Ord. 99-07 §§ 1, 2; prior code § 15-9)

10.12.025 Seasonal parking
.
The hourly parking along North Harbor Drive shall be effective from May 1st through September 30th each year. (Ord. 99-07 § 3)

10.12.030 Temporary prohibitions.

A. Notwithstanding any other provision of this title, no person may park or cause a motor vehicle to be parked, and no motor vehicle may be parked, on any street in the city upon which snow removal is undertaken by or on behalf of the city from the time that snow removal operations on the street appear to be necessary until the time that the snow removal operations on the street are completed.

B. The chief of police, or other persons designated by the city manager, is authorized to determine and designate by proper signs, places in which the stopping, standing or parking of a motor vehicle is restricted or prohibited because of traffic conditions, construction, accidents, parades, special events or other purposes deemed by the city to warrant temporary prohibitions on parking, stopping or standing. No person may park, stop or stand a motor vehicle, and no motor vehicle may be parked or stopped, in any area so designated.

C. No person may fail or refuse to immediately move his vehicle when requested to do so by a city police officer or any city employee or contractor engaged in any activity which would be hindered or obstructed in any manner if the vehicle were to remain in the place it occupied at the time the request was made. Upon request, the owner or operator of the vehicle shall move it to a location which does not interfere with the activity which was being hindered or obstructed.

D. Failure to move the vehicle upon request is a separate offense from allowing that vehicle to be parked or stopped in a prohibited area. It is not necessary that a request be made to move the vehicle before the sanctions set forth in Section 10.12.040 may be imposed. (Prior code § 15-10)

10.12.040 Penalty and impoundment.

A. Any vehicle in violation of Section 10.12.020 or 10.12.030 may be impounded by the city, or issued a traffic citation, or both.

B. A vehicle will be impounded from private property only upon the written request of the person who owns or controls the property. Before the vehicle is impounded, the city may require the person requesting the impoundment to sign a statement of ownership or control of the private property involved, and an agreement holding the city harmless for any injury, loss or damage arising from the impoundment.

C. If the vehicle is impounded from either public or private property, this impoundment is done without liability on the part of the city for any damage which may be done to it or its contents. The vehicle shall not be returned to the owner or operator thereof until any impound fees, and any storage or other charges which may have accrued, have been paid.

DD. If the vehicle is cited, the penalty for ~~the~~ violation of section 10.12.020 is fifty dollars and the penalty for violation of section 10.12.030 ~~this ordinance~~ is two-hundred ~~twenty~~ dollars.

E. If the vehicle is both impounded and cited, all impound and citation fees, and other charges, must be paid prior to the return of the vehicle to the owner or operator. (Prior code § 15-11)

Section 2. This ordinance shall take effect immediately upon adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this _____day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstain:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Walker, P.C

File #: ORD 24-0004, **Version:** 1

ITEM TITLE:
#24-04 - Amending Chapter 1.08 of the Valdez Municipal Code Titled General Penalty. First Reading. Public Hearing.

SUBMITTED BY: Sheri Pierce, MMC, City Clerk/Jake Staser, City Attorney

FISCAL NOTES:

Expenditure Required: N/A
Unencumbered Balance: N/A
Funding Source: N/A

RECOMMENDATION:

Approve Ordinance #24-04 at first reading for public hearing.

SUMMARY STATEMENT:

Ordinance #24-02 amending Chapter 10.12 of the Valdez Municipal Code including implementation of a fine schedule is under consideration by Council.

This fine schedule must be incorporated into the Minor Offense Fine Schedule established in Chapter 1.08 - General Penalty. This ordinance incorporates the “minor offense” fines adopted in Chapter 10.12.

Summary of previous action on Ordinance 24-04:

2/20/24: Initial first reading. Postponed to the next regular meeting due to drafting error in 24-02, the ordinance establishing the fine.

3/5/24: In first reading. Amended to strike $200 and insert $80, returned to first reading.

Note:

Fine amounts in Ordinance 24-02 and Ordinance 24-04 need to match.

CITY OF VALDEZ, ALASKA

ORDINANCE NO. 24-04

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA AMENDING CHAPTER 1.08 OF THE VALDEZ MUNICIPAL CODE TITLED GENERAL PENALTY

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA that:

Section 1: Chapter 1.08, Section 1.08.030 of the Valdez Municipal Code is hereby amended to read as follows:

GENERAL PENALTY

Sections:

1.08.030 Minor offense fine schedule.

In accordance with AS 29.25.070(a), citations for the following offenses may be disposed of as provided in AS 12.25.195 through 12.25.230, without a court appearance, upon payment of the fine amounts listed below to the court within thirty days of the date of the citation, plus the state surcharge required by AS 12.55.039 and 29.25.074. The Rules of Minor Offense Procedure in the Alaska Rules of Court applies to all offenses listed below. Citations charging these offenses must meet the requirements of Minor Offense Rules. If a person charged with one of these offenses appears in court and is found guilty, the penalty imposed for the offense may not exceed the fine amount for that offense listed below. If an offense is not listed on this fine schedule or another fine schedule, the defendant must appear in court to answer to the charges. These fines may not be judicially reduced.

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.010	Cleanup and disposal of animal litter or excrement required—first offense	Optional	$25.00
6.08.010	Cleanup and disposal of animal litter or excrement required—second offense	Optional	$50.00
6.08.010	Cleanup and disposal of animal litter or excrement required—third offense	Optional	$100.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.010	Cleanup and disposal of animal litter or excrement required—fourth and subsequent	Optional	$300.00
6.08.020	Animal running at large prohibited—first offense	Optional	$25.00
6.08.020	Animal running at large prohibited—second offense	Optional	$50.00
6.08.020	Animal running at large prohibited—third offense	Optional	$100.00
6.08.020	Animal running at large prohibited—fourth and subsequent	Optional	$300.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—first offense	Optional	$25.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—second offense	Optional	$50.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—third offense	Optional	$100.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—fourth and subsequent	Optional	$300.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—first offense	Optional	$50.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—second offense	Optional	$100.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—third offense	Optional	$200.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—fourth and subsequent offense	Optional	$400.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.050	Keeping of wild animals within the city prohibited—first offense	Optional	$50.00
6.08.050	Keeping of wild animals within the city prohibited—second offense	Optional	$100.00
6.08.050	Keeping of wild animals within the city prohibited—third offense	Optional	$200.00
6.08.050	Keeping of wild animals within the city prohibited—fourth and subsequent offense	Optional	$400.00
6.08.090	Continuous noise by animal prohibited—first offense	Optional	$25.00
6.08.090	Continuous noise by animal prohibited—second offense	Optional	$50.00
6.08.090	Continuous noise by animal prohibited—third offense	Optional	$100.00
6.08.090	Continuous noise by animal prohibited—fourth and subsequent offense	Optional	$300.00
6.08.100	Failure to confine female dog or cat in heat—first offense	Optional	$25.00
6.08.100	Failure to confine female dog or cat in heat—second offense	Optional	$50.00
6.08.100	Failure to confine female dog or cat in heat—third offense	Optional	$100.00
6.08.100	Failure to confine female dog or cat in heat—fourth and subsequent offense	Optional	$300.00
6.08.110	Tethering/chaining/crating of animals restricted—first offense	Optional	$50.00
6.12.010	Dog license required—first offense	Optional	$25.00
6.12.010	Dog license required—second offense	Optional	$50.00
6.12.010	Dog license required—third offense	Optional	$100.00
6.12.010	Dog license required—fourth and subsequent offense	Optional	$300.00
6.12.020	Display of license tag on dog required	Optional	$25.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.12.030	Vaccination of dogs required—first offense	Optional	$25.00
6.12.030	Vaccination of dogs required—second offense	Optional	$50.00
6.12.030	Vaccination of dogs required—third offense	Optional	$100.00
6.12.030	Vaccination of dogs required—fourth and subsequent offense	Optional	$300.00
6.12.040	Kennel licenses required—first offense	Optional	$50.00
6.12.040	Kennel licenses required—second offense	Optional	$100.00
6.12.040	Kennel licenses required—third offense	Optional	$200.00
6.12.040	Kennel licenses required—fourth and subsequent offense	Optional	$400.00
6.13.010	Excessive number of cats prohibited—first offense	Optional	$25.00
6.13.010	Excessive number of cats prohibited—second offense	Optional	$50.00
6.13.010	Excessive number of cats prohibited—third offense	Optional	$100.00
6.13.010	Excessive number of cats prohibited—fourth and subsequent offense	Optional	$300.00
6.13.020	Cattery license required—first offense	Optional	$50.00
6.13.020	Cattery license required—second offense	Optional	$100.00
6.13.020	Cattery license required—third offense	Optional	$200.00
6.13.020	Cattery license required—fourth and subsequent offense	Optional	$400.00
9.12.010	Disorderly conduct—first offense	Optional	$50.00
9.12.010	Disorderly conduct—second offense	Optional	$100.00
9.12.010	Disorderly conduct—third offense	Optional	$200.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
9.12.010	Disorderly conduct—fourth and subsequent	Optional	$400.00
9.12.030	Loitering on school grounds—first offense	Optional	$50.00
9.12.030	Loitering on school grounds—second offense	Optional	$100.00
9.12.030	Loitering on school grounds—third offense	Optional	$200.00
9.12.030	Loitering on school grounds—fourth and subsequent	Optional	$400.00
9.12.070(A) and (B)	Use of fireworks outside of permitted times prohibited	Optional	$100.00
9.12.070(C) and (D)	Negligent use of fireworks or use while under influence prohibited	Optional	$300.00
9.20.010(H) and (I)	Harvesting of trees without permit prohibited—first offense	Optional	$50.00
9.20.010(H) and (I)	Harvesting of trees without permit prohibited—second and subsequent	Optional	$100.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—first offense	Optional	$300.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—second offense	Optional	$400.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—third and subsequent	Optional	$500.00
9.32.010	Discharge of firearms—first offense	Optional	$100.00
9.32.010	Discharge of firearms—second offense	Optional	$200.00
9.32.010	Discharge of firearms—third offense	Optional	$300.00
9.32.010	Discharge of firearms—fourth and subsequent offense	Optional	$500.00
10.12.020	Parking prohibited in specific areas	Optional	$50.00
10.12.030	Temporary prohibitions on parking	Optional	$200.00

Section 2: This ordinance shall take effect immediately following final approval and adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA this _____ day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstaining:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Walker, P.C.

CITY OF VALDEZ, ALASKA

ORDINANCE NO. 24-04

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA AMENDING CHAPTER 1.08 OF THE VALDEZ MUNICIPAL CODE TITLED GENERAL PENALTY

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA that:

Section 1: Chapter 1.08, Section 1.08.030 of the Valdez Municipal Code is hereby amended to read as follows:

GENERAL PENALTY

Sections:

1.08.030 Minor offense fine schedule.

In accordance with AS 29.25.070(a), citations for the following offenses may be disposed of as provided in AS 12.25.195 through 12.25.230, without a court appearance, upon payment of the fine amounts listed below to the court within thirty days of the date of the citation, plus the state surcharge required by AS 12.55.039 and 29.25.074. The Rules of Minor Offense Procedure in the Alaska Rules of Court applies to all offenses listed below. Citations charging these offenses must meet the requirements of Minor Offense Rules. If a person charged with one of these offenses appears in court and is found guilty, the penalty imposed for the offense may not exceed the fine amount for that offense listed below. If an offense is not listed on this fine schedule or another fine schedule, the defendant must appear in court to answer to the charges. These fines may not be judicially reduced.

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.010	Cleanup and disposal of animal litter or excrement required—first offense	Optional	$25.00
6.08.010	Cleanup and disposal of animal litter or excrement required—second offense	Optional	$50.00
6.08.010	Cleanup and disposal of animal litter or excrement required—third offense	Optional	$100.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.010	Cleanup and disposal of animal litter or excrement required—fourth and subsequent	Optional	$300.00
6.08.020	Animal running at large prohibited—first offense	Optional	$25.00
6.08.020	Animal running at large prohibited—second offense	Optional	$50.00
6.08.020	Animal running at large prohibited—third offense	Optional	$100.00
6.08.020	Animal running at large prohibited—fourth and subsequent	Optional	$300.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—first offense	Optional	$25.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—second offense	Optional	$50.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—third offense	Optional	$100.00
6.08.040(A)(1)	Negligent feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—fourth and subsequent	Optional	$300.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—first offense	Optional	$50.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—second offense	Optional	$100.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—third offense	Optional	$200.00
6.08.040(A)(2)	Intentional feeding of wild animals, birds of prey, or deleterious exotic wildlife prohibited—fourth and subsequent offense	Optional	$400.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.08.050	Keeping of wild animals within the city prohibited—first offense	Optional	$50.00
6.08.050	Keeping of wild animals within the city prohibited—second offense	Optional	$100.00
6.08.050	Keeping of wild animals within the city prohibited—third offense	Optional	$200.00
6.08.050	Keeping of wild animals within the city prohibited—fourth and subsequent offense	Optional	$400.00
6.08.090	Continuous noise by animal prohibited—first offense	Optional	$25.00
6.08.090	Continuous noise by animal prohibited—second offense	Optional	$50.00
6.08.090	Continuous noise by animal prohibited—third offense	Optional	$100.00
6.08.090	Continuous noise by animal prohibited—fourth and subsequent offense	Optional	$300.00
6.08.100	Failure to confine female dog or cat in heat—first offense	Optional	$25.00
6.08.100	Failure to confine female dog or cat in heat—second offense	Optional	$50.00
6.08.100	Failure to confine female dog or cat in heat—third offense	Optional	$100.00
6.08.100	Failure to confine female dog or cat in heat—fourth and subsequent offense	Optional	$300.00
6.08.110	Tethering/chaining/crating of animals restricted—first offense	Optional	$50.00
6.12.010	Dog license required—first offense	Optional	$25.00
6.12.010	Dog license required—second offense	Optional	$50.00
6.12.010	Dog license required—third offense	Optional	$100.00
6.12.010	Dog license required—fourth and subsequent offense	Optional	$300.00
6.12.020	Display of license tag on dog required	Optional	$25.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
6.12.030	Vaccination of dogs required—first offense	Optional	$25.00
6.12.030	Vaccination of dogs required—second offense	Optional	$50.00
6.12.030	Vaccination of dogs required—third offense	Optional	$100.00
6.12.030	Vaccination of dogs required—fourth and subsequent offense	Optional	$300.00
6.12.040	Kennel licenses required—first offense	Optional	$50.00
6.12.040	Kennel licenses required—second offense	Optional	$100.00
6.12.040	Kennel licenses required—third offense	Optional	$200.00
6.12.040	Kennel licenses required—fourth and subsequent offense	Optional	$400.00
6.13.010	Excessive number of cats prohibited—first offense	Optional	$25.00
6.13.010	Excessive number of cats prohibited—second offense	Optional	$50.00
6.13.010	Excessive number of cats prohibited—third offense	Optional	$100.00
6.13.010	Excessive number of cats prohibited—fourth and subsequent offense	Optional	$300.00
6.13.020	Cattery license required—first offense	Optional	$50.00
6.13.020	Cattery license required—second offense	Optional	$100.00
6.13.020	Cattery license required—third offense	Optional	$200.00
6.13.020	Cattery license required—fourth and subsequent offense	Optional	$400.00
9.12.010	Disorderly conduct—first offense	Optional	$50.00
9.12.010	Disorderly conduct—second offense	Optional	$100.00
9.12.010	Disorderly conduct—third offense	Optional	$200.00

MUNICIPAL CODE SECTION	OFFENSE DESCRIPTION	COURT APPEARANCE	PENALTY/FINE
9.12.010	Disorderly conduct—fourth and subsequent	Optional	$400.00
9.12.030	Loitering on school grounds—first offense	Optional	$50.00
9.12.030	Loitering on school grounds—second offense	Optional	$100.00
9.12.030	Loitering on school grounds—third offense	Optional	$200.00
9.12.030	Loitering on school grounds—fourth and subsequent	Optional	$400.00
9.12.070(A) and (B)	Use of fireworks outside of permitted times prohibited	Optional	$100.00
9.12.070(C) and (D)	Negligent use of fireworks or use while under influence prohibited	Optional	$300.00
9.20.010(H) and (I)	Harvesting of trees without permit prohibited—first offense	Optional	$50.00
9.20.010(H) and (I)	Harvesting of trees without permit prohibited—second and subsequent	Optional	$100.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—first offense	Optional	$300.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—second offense	Optional	$400.00
9.24.070	Sale of tobacco to children under nineteen years of age prohibited—third and subsequent	Optional	$500.00
9.32.010	Discharge of firearms—first offense	Optional	$100.00
9.32.010	Discharge of firearms—second offense	Optional	$200.00
9.32.010	Discharge of firearms—third offense	Optional	$300.00
9.32.010	Discharge of firearms—fourth and subsequent offense	Optional	$500.00
10.12.020	Parking prohibited in specific areas	Optional	$50.00
10.12.030	Temporary prohibitions on parking	Optional	$80.00

Section 2: This ordinance shall take effect immediately following final approval and adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA this _____ day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstaining:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Walker, P.C.

File #: ORD 24-0005, **Version:** 1

ITEM TITLE:
#24-05 - Amending Chapter 3.24 of the Valdez Municipal Code Titled Public Accommodation Tax. Second Reading. Adoption.

SUBMITTED BY: Jake Staser, City Attorney/ Elise Sorum-Birk, Deputy City Clerk

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Approve Ordinance 24-05 Amending Chapter 3.24 of the Valdez Municipal Code Titled Public Accommodation Tax. Second Reading. Adoption.

SUMMARY STATEMENT:

With passage of Ordinance 24-01, amending the city's zoning code, there is a need to clarify Chapter 3.24 of the Valdez Municipal Code relating to public accommodation taxes and short term rentals.

This ordinance does the following:

- Narrows the existing definition of "public accommodation" to cover only rentals of 30 day or fewer and to align with definitions of "short term rental" and "hotel, motel, inn or lodge" in the updated title 17.
    - Currently this code's definition includes all manner of structure and facility rented for a period of 6 months or fewer.
- Defines "hosting platform" and requires these online platforms to register with the city and remit taxes on behalf of operators who use them.
- Simplifies registration process for operators.
- Clarifies that all public accommodation operators must follow the other provisions of the code to maintain their registration.
- Removes language referencing specific months of the fiscal year in relation to distribution of funds.

The intent of these changes is administrative in nature and aims to make collection of public

accommodation tax on short term rentals less onerous for both new operators and the city.

CITY OF VALDEZ, ALASKA

ORDINANCE NO. 24-05

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, AMENDING CHAPTER 3.24 OF THE VALDEZ MUNICIPAL CODE TITLED PUBLIC ACCOMMODATION TAX

WHEREAS, short-term vacation rental businesses have become prevalent and popular in Valdez; and

WHEREAS, with adoption of Ordinance 24-01, updating the city's zoning code, these short-term rental businesses are now able to legally operate in the city; and

WHEREAS, there is a need to ensure that the definitions adopted in the new Title 17 of Valdez Municipal Code are consistently applied throughout other titles of the Valdez Municipal Code; and

WHEREAS, the United States Supreme Court held in South Dakota v. Wayfair, Inc. that a physical presence in a taxing jurisdiction is no longer required for an entity to have a substantial nexus with the jurisdiction allowing local and state taxing authorities to require online hosting platforms to remit local taxes (without an agreement); and

WHEREAS, this ordinance will require all hosting platforms to register, collect, and remit public accommodation tax on behalf of the operators for guests using the platform.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA that the following amendments are made to Chapter 3.24 of the Valdez Municipal Code:

Section 1. Chapter 3.24 of the Valdez Municipal Code is hereby amended to read as follows:

Chapter 3.24

PUBLIC ACCOMMODATION TAX

Sections:

3.24.010 Definitions.
3.24.020 Levied—Responsibility for payment—Collection.
3.24.030 ~~Certificate of r~~ Registration for operators.
3.24.032 Registration for hosting platforms.
3.24.040 Receipts—Segregation.
3.24.050 Receipts—Transmittal—Due date—Penalty.
3.24.060 Returns to be confidential.
3.24.070 Records—Maintenance and inspection.

3.24.080 Records—Investigation by city.
3.24.090 Suits for collection.
3.24.100 Prohibited acts.
3.24.110 Civil penalties for violations.
3.24.120 Distribution of funds.

3.24.010 Definitions.

For the purposes of this chapter, the following words and phrases shall have the meanings respectively ascribed to them by this section:

"Guest" means an individual, corporation, partnership or association paying or agreeing to pay monetary consideration for the use of a public accommodation.

"Hosting platform" means a person or entity that provides a means through which an operator may offer a public accommodation for rent, usually through an online platform that provides a means for the guest to pay rent for a public accommodation.

"Operator" means a person who furnishes or offers for rent a public accommodation in the city for monetary consideration, whether acting directly or through an agent or employee.

"Person" means an individual and entities recognized by law.

"Public accommodation" means a ~~structure, facility or portion of a structure or facility which is occupied, or intended and designed for occupancy by guests for dwelling, lodging, or sleeping purposes and includes any construction camp, hotel, motel, apartments within a hotel/motel unless the apartments are under lease to the same person/company for a minimum period of six months, inn, boarding house, bed and breakfast home, vessel or similar structure or facility.~~ "Hotel, Motel, Inn or Lodge" or "Short-term rental" as defined in Title 17 of this code.

"Quarter" means computed by use of the calendar year beginning with January and consisting of a three-month period.

"Rents" means the amount paid as monetary consideration for the use of a public accommodation by a guest. (Ord. 94-06 § 1: Ord. 94-02 § 1 (part): prior code § 25-126)

3.24.020 Levied—Responsibility for payment—Collection.

A. The city levies a tax on public accommodation rentals within the city equal to six percent of the rental. The tax shall be applicable to all rentals, unless the rental is specifically exempt from taxation, as follows:

1. Rent paid directly by the United States or state of Alaska insofar as they are immune from taxation;

2. An employee of the public accommodation collecting the tax.

B. Each guest is responsible for the tax imposed by this chapter, and the tax shall be due and payable at the time the rent is paid. If the rent is paid in installments, a proportionate share

of the tax shall be paid with each installment. The unpaid tax shall be due when the guest ceases to occupy or use space in the public accommodation.

C. Every operator renting a public accommodation subject to taxation under this chapter shall collect the taxes imposed by this chapter from the guest at the time of collection of the rental and shall transmit the same quarterly to the city unless taxes imposed by this chapter are collected by a hosting platform. The tax imposed shall be shown on the billing to the guest as a separate and distinct item. (Ord. 94-02 § 1 (part): prior code § 25-127)

D. Every hosting platform accepting public accommodation rental payment from a guest on behalf of an operator as defined in this chapter shall collect the taxes imposed by this chapter from the guest at the time of collection of the rental payment and shall remit all public accommodation taxes collected to the city on a quarterly basis.

3.24.030 ~~Certificate of~~ r Registration for operators.

A. Operators shall register with the city by providing the approved business registration for the public accommodation and, if required, the short term rental permit prior to commencing business. ~~apply to the city for a certificate of registration not later than ten days from the effective date of the ordinance codified in this chapter, the date of commencement of business or the opening of additional places of business. Upon receipt of a properly executed application, and approval of a city business registration, the city may issue a certificate of registration to the operator authorizing the operator to collect the tax at the business address stated on the certificate.~~

B. The city finance department shall maintain a record of all registered operators authorized to collect and remit public accommodation taxes. ~~certificate must be displayed prominently at the registered place of business.~~

C. Operators shall provide the city finance department written notice in the event of a change of business type, change of address or closing of a public accommodation business. ~~The certificate of registration is nonassignable and nontransferable and must be surrendered to the city by the operator to whom it was issued upon the operator's cessation of the business at the location stated in the certificate. If the business is continued at the same location but the form of business organization is changed, the operator shall surrender the old certificate to the city for cancellation. The new operator shall file a new application for the certificate of registration and, upon receipt of a properly executed application, and approval of a city business registration, a new certificate will be issued. If there is a change of address for the operator's place of business, a new certificate of registration is required showing the new location or address.~~

D. For a registration to be valid the operator must comply with Valdez business registration requirements as well as the provisions of the zoning, building, plumbing, electrical, and fire codes, and other applicable ordinances of the city. (Ord. 94-02 § 1 (part): prior code § 28-128)

3.24.035 Registration for hosting platforms

A. Every hosting platform accepting payment for public accommodation rentals as defined by this chapter shall register with the city upon a form provided by the city. There is no requirement for a hosting platform to hold a city business registration or have a physical presence within the city.

B. The city finance department shall maintain a record of registered hosting platforms authorized to collect and remit public accommodation taxes.

3.24.040 Receipts—Segregation.

Title to the taxes collected pursuant to this chapter shall vest to the city upon collection. Such taxes shall be segregated by the operator or hosting platform from the funds of the operator or hosting platform ~~public accommodation~~ and safeguarded until transmitted to the city as hereinafter provided. (Ord. 94-02 § 1 (part): prior code § 25-129)

3.24.050 Receipts—Transmittal—Due date—Penalty.

A. On or before the last day of the month following each calendar quarter, each operator shall prepare and submit to the city a return for the preceding quarter upon forms furnished by the city setting forth the amount received for:

1. Rentals within the city;

2. Taxes collected.

In addition, the operator shall submit such other information and supporting papers as may be required by the city.

B. The operator shall sign the return and transmit it together with the taxes collected to the city on or before the due date. A return shall be filed even if the public accommodation has no rental for the quarter.

C. Taxes collected by an operator as provided by this chapter shall be due the last day of the month following each calendar quarter. If taxes collected by an operator have not been received by the city on or before the due date, the operator shall incur a penalty equal to ten and one-half percent of the taxes which are due or a minimum of one hundred dollars and shall be charged interest at the rate of ten and one-half percent per annum for each day the tax is delinquent. A one-time-only waiver of penalty will be given for any late filed tax return after April 30, 1994.

D. Where the city has reasonable grounds to believe that taxes due were not collected or taxes collected were not transmitted on or before the due date, or if the operator of a public accommodation has failed to file a return as required by this chapter, the city shall prepare a notice of delinquency and shall deliver such notice to the operator. Payment of delinquent tax under a notice of delinquency shall include penalty and interest which shall be calculated as provided above.

E. A registered hosting platform shall submit tax returns and remit tax payments in accordance with this section. The tax return shall set forth or include the aggregate amounts of all rents earned by and taxes due from the operators who use the hosting platform to rent or offer to rent public accommodations through the hosting platform. To the extent a hosting platform collects taxes on behalf of an operator, the operator's liability for those taxes shall be deemed satisfied. (Ord. 94-02 § 1 (part): prior code § 25-130)

3.24.060 Returns to be confidential.

All returns filed with the city pursuant to the provisions of this chapter and all data obtained from such returns are confidential and may not be released for inspection by the public, except upon court order. (Ord. 94-02 § 1 (part): prior code § 25-131)

3.24.070 Records—Maintenance and inspection.

A. Regardless of whether a hosting platform is used, e~~E~~very operator of a public accommodation engaged in business within the city shall keep and preserve suitable records of all rentals made and such other books and accounts as may be necessary to determine the amount of tax required to be collected. All books, invoices and other necessary records shall be maintained by the operator for a period of two years and shall be available for examination at reasonable times by the city for the purpose of ascertaining the correctness of a return or for the purpose of determining the amount of tax collected or levied.

B. A registered hosting platform shall keep and preserve suitable records of all rental transactions subject to this chapter and all claimed exemptions from payment, collection, or remittance of the public accommodation taxes under this chapter. To the extent a hosting platform may assign anonymous account numbers to operators using the hosting platform, when inspecting records, the city shall inspect the required records in an anonymized fashion, unless the city has obtained a release of information from the operator or an order to produce identifiable operator information issued through a binding legal process. (Ord. 94-02 § 1 (part): prior code § 25-133)

3.24.080 Records—Investigation by city.

The city may conduct investigations and hearings concerning any matters covered by this chapter, may examine relevant books, papers, records or memoranda of any operator and may require the attendance of the operator, his officers or employees. The city shall have the power to administer oaths to persons testifying, and may issue formal subpoenas to compel attendance or to require production of relevant books, papers, records or memoranda. All subpoenas issued under the terms of this chapter may be served on any person of legal age. The fees paid to witnesses for attendance at the hearings shall be the same as the fees paid to witnesses before the Superior Court, and such fees shall be paid when the witness is excused from further attendance. When a witness is subpoenaed at the insistence of any party to the proceeding, the cost of service of the subpoena and the fee of the witness shall be borne by the party at whose request the witness is summoned. A subpoena shall be served in the same

manner as a subpoena issued by a Superior Court. The city or any party to an investigation or hearing before the city may cause the deposition of witnesses residing within or without the state to be taken in a manner prescribed by law for depositions in civil actions in the courts of this state and to that end may compel the attendance of witnesses and production of relevant books, papers, records or memoranda.

3.24.090 Suits for collection.

Taxes due but not paid or taxes collected but not transmitted may be recovered in an action at law against the guest or the public accommodation operator. Tax returns shall be prima facie proof of taxes collected but not transmitted. (Ord. 94-02 § 1 (part): prior code § 25-134)

3.24.100 Prohibited acts.

A. No person may fail or refuse to pay the tax imposed by this chapter when it is due and payable to an operator authorized to collect the tax.

B. An operator or hosting platform may not advertise or state to the public or to any guest directly or indirectly that the tax or any part of it will be assumed or absorbed by the operator or hosting platform, or that the tax will not be added to the rental or that it will be refunded. An operator or hosting platform may not absorb or fail to add the tax or any part of it or refund any tax or fail to state the tax separately to the guest. (Ord. 94-02 § 1 (part): prior code § 25-135)

3.24.110 Civil penalties for violations.

An operator who rents accommodations in the city and who thereafter fails to file a tax return as required by this chapter shall incur civil penalty equal to ten percent of the taxes due to the city for each quarter for which a return was not filed as required by this chapter. An operator who, in the course of business, rents accommodations upon which a tax is levied hereunder and who fails to collect such a tax shall incur a civil penalty of double the tax which should have been collected. A hosting platform that collects public accommodation taxes on behalf of an operator is subject to the penalties set forth herein. In addition, a violator of this chapter is subject to criminal penalties as set forth in Section 1.08.010 of this code. (Ord. 94-02 § 1 (part): prior code § 25-136)

3.24.120 Distribution of funds.

A. Funds received under this chapter including penalties and interest for each calendar year may be available for use as follows:

1. Up to one hundred percent of the gross funds may be made available for distribution. The cost of administration and collection of the public accommodation tax shall come from the gross funds prior to distribution.

2. Funds available for distribution shall be those public accommodation tax funds received by the city during the prior fiscal year. ~~from April 1st through December 31st and the current fiscal year from January 1st through March 31st.~~

3. All public accommodation tax funds received under this chapter will be placed in an economic development fund and will be distributed at the discretion of the city council.

4. Each applicant for funds shall submit a program description including, but not limited to, the following:

a. Program objectives;

b. Economic development benefit or opportunities;

c. Annual operating budget; and

d. Financial statement including revenues, expenditures and reserve account balances.

The submission date will be determined on an annual basis by the city manager. (Ord. 04-10: Ord. 02-07 § 1; Ord. 99-13 § 1: Ord. 94-02 § 1 (part): prior code § 25-137)

Section 2. This ordinance shall take effect immediately upon adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this _____day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Elise Sorum-Birk, Deputy City Clerk

APPROVED AS TO FORM:

_____
Jake Stasser, City Attorney
Brena, Bell, & Clarkson, P.C

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstain:

File #: ORD 24-0006, **Version:** 1

ITEM TITLE:
#24-06 - Amending Title 6 of the Valdez Municipal Code by Amending Section 6.04.010 Titled Definitions and Section 6.08.020 Titled Running at Large. Second Reading. Adoption.

SUBMITTED BY: Elise Sorum-Birk, Deputy City Clerk/ Jake Staser, City Attorney

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Approve Ordinance 24-06 in second reading for adoption.

SUMMARY STATEMENT:

Ordinance 24-06 is attached.

The aim of this amendment to Title 6 is to create a codified process for the establishment of off-leash areas within Valdez City Limits (currently off-leash areas just coincide with where firearm discharge is allowed). Additionally, the ordinance also defines “under control” in the definitions section of Title 6.

CITY OF VALDEZ, ALASKA

ORDINANCE NO. 24-06

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, AMENDING TITLE 6 OF THE VALDEZ MUNICIPAL CODE BY AMENDING SECTION 6.04.010 TITLED DEFINITIONS AND SECTION 6.08.020 TITLED RUNNING AT LARGE

WHEREAS, there is a need to define “under control” and “off-leash area” in Title 6 of the Valdez Municipal code to promote safety of dogs and their owners; and

WHEREAS, off-leash areas can promote good canine physical health and positive socialization among dogs and their owners; and

WHEREAS, there is a desire to have off-leash areas established by the city council and maps of the areas easily accessible to the public.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, that the following amendments are made to Title 6 of the Valdez Municipal Code:

Section 1. Section 6.04.010 of the Valdez Municipal Code is amended as follows:

6.04.010 Definitions.

For the purposes of this title, the following words and phrases shall have the meanings respectively ascribed to them by this section:

“Abandon” means intentionally, knowingly, recklessly or with criminal negligence leaving an animal at a location where it will not be provided proper food, water, shelter and care in a manner which might cause harm to the animal.

“Animal” means a vertebrate, living creature, not a human being, not including fish but including fowl.

“Animal control officer” means the individual designated “animal control officer” by the chief of police, or if none has been designated, the chief of police.

“Animal shelter” means the city facility for the keeping of animals impounded or otherwise taken into custody under this chapter.

“At large” means an animal that is not under restraint.

“Birds of prey” means eagles, hawks, owls, falcons, and other.

“Cattery” means a location designated for the keeping or harboring of more than four but not to exceed ten cats that are four months of age or older.

“Chief” means the chief of the Valdez police department.

"Dangerous animal" means an animal which without provocation has inflicted injury on a person or another animal on public or private property. The following exceptions, however, shall apply:

1. No animal may be declared dangerous if any injury or damage is sustained by a person who, at the time the injury or damage was sustained, was committing an unlawful trespass or other tort upon the premises occupied by the owner or keeper of the animal, or was testing, tormenting, abusing or assaulting the animal, or was committing or attempting to commit a crime.

2. No dog may be declared dangerous if the dog was protecting or defending a person within the immediate vicinity of the dog from an unjustified attack or assault.

3. No dog may be declared dangerous if the injury or damage to a domestic animal was sustained while the dog was working as a hunting dog, herding dog or predator control dog on the property of, or under the control of, its owner, and the damage or injury was to a species or type of domestic animal appropriate to the work of the dog.

4. No dog shall be declared dangerous if the dog has been trained to attack persons independently or upon oral command while under the control and supervision of an authorized government or law enforcement unit and the act is directly associated with the proper execution of its duties.

"Deleterious exotic wildlife" means any starling, English sparrow, or raccoon; any Muridae rodent (to include true mice and rats, gerbils, and their relatives), rockdove or Belgian hare that is unconfined or unconstrained; and any feral ferret or feral swine, or feral domestic rabbit.

"Department" means the Valdez police department.

"Dog" means both male and female dogs, including both domestic and wild canines.

"Fowl" means any bird, including the larger domestic birds such as chicken, duck, goose, turkey, etc.

"Hybrid animal" means an animal that is an offspring of a domesticated animal and a wild animal.

"Injury" means to damage, harm or cause pain and suffering.

"Kennel" means a facility operated by a person engaged in the commercial buying, selling, training, keeping or boarding of dogs for profit, or a facility designed for the keeping or harboring of six or more dogs that are over three months old.

"Livestock" means generally accepted outdoor farm animals such as goats, horses, pigs, barnyard fowl, etc., not to include cats, dogs and other house pets.

"Off Leash Area" means an area established, by resolution of the city council, as being an area where dogs are permitted to be off leash, provided that they are under control.

"Officer" means the animal control officer, any deputy animal control officer, or any police officer.

"Owner" means any person owning, keeping, harboring, caretaking or having custody or control of an animal.

“Pet shop” means a place or vehicle in or on which any dogs, cats, rodents, reptiles, fish, pet birds, exotic birds or exotic animals not born and raised on those premises are kept for the purpose of sale to the public.

“Provocation” means conduct which is directed by a person or an animal towards an animal that may reasonably be expected to arouse fear, rage, protective instinct or fury in the animal. Any animal which is at large cannot be considered to be provoked by an animal under restraint.

“Restraint” means and includes physical confinement, as by leash, chain, fence or building.

“Sanitary living conditions” means the animal’s living area is reasonably clear of excrement and standing water. The area is clear of broken glass, trash, nails and other items that may cause injury or death to the animal.

"Under control" means competent voice, signal or physical control that restrains an animal from approaching a bystander, from entering private property, and from causing damage to property. An animal is presumed not to have been under control if injury, damage or trespass has occurred.

“Vicious animal” means and includes:

1. An animal which when unprovoked has ever bitten or attacked a human being, serious enough to require treatment by a medical professional, without provocation on public or private property; or

2. An animal in violation of Section 6.08.060 which has been previously adjudged by a court to be dangerous.

“Wild animals” means moose, bear, coyote, wolverine, fox, or other wild mammals. (Ord. 19-04 § 1 (part): Ord. 18-01 § 1 (part): Ord. 09-07 § 1 (part): Ord. 07-07 § 1: Ord. 00-09 § 1; Ord. 93-20 § 1: prior code § 4-1)

Section 2. Section 6.08.020 of the Valdez Municipal Code is amended as follows:

6.08.020 Running at large prohibited.

A. No owner or caretaker shall fail to properly restrain his/her animal to prevent it from running at large. When an animal is found running at large, an officer under this title is authorized to impound the animal and/or give its owner or caretaker a written warning or an animal at large citation.

B. If any dangerous or vicious animal cannot be safely impounded or if any animal attacks an officer attempting to impound it, any officer may take whatever action is necessary to safeguard life and property endangered by the animal.

C. Notwithstanding the foregoing provisions of this section, dogs may run freely under control by the owner or caretaker in any area of the city designated as an off-leash area. Off-leash areas shall be established by resolution of the city council. ~~in which both hunting and the discharge of firearms is permitted~~.

D. No person other than an officer performing his/her duty may release an animal from restraint without the owner’s permission, except to preserve the animal’s life. (Ord. 19-04 § 1

(part): Ord. 18-01 § 2 (part): Ord. 09-07 § 2 (part): Ord. 00-09 § 5: Ord. 93-20 § 3: prior code § 4-11).

Section 3. This ordinance shall take effect immediately upon adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this _____day of _____, 2024.

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

First Reading:
Second Reading:
Adoption:
Ayes:
Noes:
Absent:
Abstain:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Clarkson, P.C

File #: ORD 24-0008, **Version:** 1

ITEM TITLE:
#24-08 - Amending Chapter 6.20 of the Valdez Municipal Code Titled Rabies. Second Reading. Adoption.

SUBMITTED BY: Jake Staser, City Attorney/ Elise Sorum-Birk, Deputy City Clerk

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Approve Ordinance 24-08 in second reading for adoption.

SUMMARY STATEMENT:

Ordinance 24-08 is attached.

This ordinance clarifies quarantine requirements in the case of dog bite incidents and specifically addresses the process for when an animal's owner resides outside of city limits.

CITY OF VALDEZ, ALASKA
ORDINANCE NO. 24-08

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, AMENDING CHAPTER 6.20 OF THE VALDEZ MUNICIPAL CODE TITLED RABIES

WHEREAS, there is a desire to protect public health and welfare; and

WHEREAS, there is a need to ensure that proper quarantine requirements are in place in the event of a bite from an unvaccinated dog.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA that the following amendments be made to Chapter 6.20 of the Valdez Municipal Code.

Section 1. Chapter 6.20 is amended to read as follows:

Chapter 6.20
RABIES

Sections:

6.20.010 Proclamation of emergency requiring confinement of animals.
6.20.020 Quarantine measures—Animals suspected of having rabies.
6.20.030 Quarantine measures—Animals biting persons.
6.20.040 Quarantine measures—Removal of animals with rabies prohibited—Disposition of animals with rabies.

6.20.010 Proclamation of emergency requiring confinement of animals.

Whenever it becomes necessary to safeguard the public from the dangers of hydrophobia or other disease, the city council, if they deem it necessary, shall issue a proclamation ordering every person owning or keeping an animal to confine it securely indoors unless such animal shall have a muzzle of sufficient strength to prevent it from biting any person or thing. Any unmuzzled animal running at large during the time of the proclamation shall be seized and impounded, unless noticeably infected with rabies. All animals noticeably infected with rabies and all unlicensed dogs at large during the period of such proclamation shall be immediately killed upon being apprehended. (Ord. 18-01 § 6 (part): prior code § 4-41)

6.20.020 Quarantine measures—Animals suspected of having rabies.

If an animal is believed to have rabies, or has been bitten by an animal suspected of having rabies, such animal shall be confined indoors or muzzled and confined by a leash or chain on the owner's premises and shall be placed under the observation of a duly licensed physician or veterinarian licensed under Alaska Statute 08.98 for two weeks at the expense of the owner. The owner shall notify ~~the department~~ the animal control officer of the fact that his animal has been possibly exposed or exposed to rabies and~~, at his discretion,~~ the animal control officer is empowered to have such animal removed from the owner's premises and placed under observation for two weeks at the expense of the owner. (Ord. 18-01 § 6 (part): prior code § 4-42)

6.20.030 Quarantine measures—Animals biting persons.

A. ~~No animal shall bite persons or other animals. Whenever any~~ If an animal bites a person:

1. The bitten person ~~so bitten~~ and the owner of the animal shall immediately notify the police department which shall order the animal held on the owner's premises, or shall have it impounded as long as necessary for a complete examination at the Valdez animal shelter for not less than ten days. The animal's owner or caretaker shall be responsible for the daily maintenance fee.

2. A physician or other practitioner of medicine who treats a person for an animal bite shall report the incident to the Valdez animal control or the Valdez police department and must release the name and address of the person being treated and any other information that may aid in the control of rabies.

3. A physical examination of the quarantined animal is to be made by a ~~duly licensed~~ veterinarian licensed under Alaska Statute 08.98 or the department's animal control officer at the end of the quarantine period to check the animal for any signs of disease.

    a. If it is determined by ~~a duly licensed~~ veterinarian licensed under Alaska Statute 08.98 that the animal is infected with rabies or other dangerous, contagious, and infectious disease, it shall be the

duty of the animal control officer to ~~destroy such animal in as humane a manner as is reasonably possible~~ ensure the animal is euthanized.

b. An animal shall be released from quarantine only when it is determined by the animal control officer or ~~a duly licensed~~ veterinarian licensed under Alaska Statute 08.98, with written proof provided to the animal control officer, that the animal is free from such a disease.

4. The owner or persons harboring an animal under quarantine shall immediately notify animal control if such an animal becomes sick or dies during its period of confinement. If the animal dies during the period of quarantine or impoundment, its head shall be sent to the State Department of Health ~~and Social Services~~ laboratory for examination.

5. During the period of quarantine, it shall be unlawful to remove the animal from the Valdez city limits.

6. Any animal whose owner resides outside of the Valdez city limits shall be quarantined at the animal shelter.

7. Prior to release from quarantine the animal must be vaccinated for rabies if it did not have the vaccination prior to the quarantine.

8. After the quarantine has ended, the owner shall be notified. If the animal is not claimed by the owner within five days, during which the animal shelter is open for regular business, the animal shall become property of the city. The owner shall be responsible for the daily maintenance fee for any day after the quarantine has ended.

B. As a result of the ineffectiveness of the rabies vaccine on hybrids, any animal that is purported to be hybrid shall not be placed into quarantine. ~~Such~~ Hybrid animals shall be immediately and ~~humanely~~ euthanized and submitted to the Department of Health ~~and Social Services~~ or a laboratory designated by the department for rabies testing. This practice is in accordance with the policy of the State of Alaska Department of Health ~~and Social Services~~, Section of Epidemiology and 7 AAC 27.020. (Ord. 18-01 § 6 (part): Ord. 00-09 § 14: prior code § 4-43)

6.20.040 Quarantine measures—Removal of animals with rabies prohibited—Disposition of animals with rabies.

No person, knowing or suspecting that an animal has rabies, shall allow ~~such~~ the animal to be taken off ~~his~~ the premises or beyond the Valdez city limits without the written permission of the animal control officer. Every owner or other person upon ascertaining an animal is rabid shall immediately notify the ~~department~~ animal control officer. ~~and such~~ The animal shall be ~~either immediately killed or removed to the animal shelter~~ euthanized. (Ord. 18-01 § 6 (part): prior code § 4-44)

Section 2. This ordinance shall take effect immediately following adoption by the Valdez City Council.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this _____day of _____, 2024

CITY OF VALDEZ, ALASKA

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

Adoption:
Yeas:
Noes:
Absent:
Abstaining:

APPROVED AS TO FORM:

_____
Jake Staser, City Attorney
Brena, Bell, & Walker, P.C.

File #: RES 24-0008, **Version:** 1

ITEM TITLE:
#24-08 - Authorizing the Submission of a Local Cybersecurity Grant through the Alaska Division of Homeland Security and Emergency Management to Develop a Cybersecurity Assessment

SUBMITTED BY: Matthew Osburn, IT Director

FISCAL NOTES:

Expenditure Required: NA
Unencumbered Balance: NA
Funding Source: NA

RECOMMENDATION:

Approve Resolution 24-07.

SUMMARY STATEMENT:

This grant application would fund an IT assessment to identify potential risks and vulnerabilities in the City's technology infrastructure, evaluate the effectiveness of current IT operations, and identify opportunities to improve performance, security, and efficiency.

CITY OF VALDEZ, ALASKA

RESOLUTION #24-08

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, AUTHORIZING THE SUBMISSION OF A LOCAL CYBERSECURITY GRANT THROUGH THE ALASKA DIVISION OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT TO DEVELOP A COMPREHENSIVE CYBERSECURITY ASSESSMENT

WHEREAS, the State of Alaska Division of Homeland Security and Emergency Management administers the State and Local Cybersecurity Grant Program (SLCGP) on behalf on the U.S. Department of Homeland Security; and

WHEREAS, the State of Alaska will be focusing on providing cost-effective and scalable cybersecurity services to local governments, including supporting the establishment of risk assessment protocols for local governments; and

WHEREAS, a cybersecurity risk assessment evaluates an organization's vulnerabilities and threats to identify the risks it faces and includes recommendations for mitigating those risks; and

WHEREAS, cybersecurity risk assessments help organizations to identify and prioritize areas for improvement in their cybersecurity program and also help organizations to communicate their risks to stakeholders and make informed decisions about how to allocate resources to reduce those risks; and

WHEREAS, a risk estimation and evaluation are usually performed, followed by the selection of controls to treat the identified risks; and

WHEREAS, it is important to continually monitor and review the risk environment to detect any changes in the context of the organization, and to maintain an overview of the complete risk management process; and

WHEREAS, the City of Valdez plans to apply for a grant up to $80,000 in funding to support development of a risk assessment; and

WHEREAS, there is a 20% local match requirement of $16,000 that may be provided by the State of Alaska, but will be required from the City should state funding not be available.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, that:

The City Manager of the City of Valdez is authorized by Valdez City Council to submit a grant application to the Alaska Division of Homeland Security for a Local

Cybersecurity Grant in the amount of $80,000, with a potential city match of $16,000 for a total project cost of $80,000.

PASSED AND APPROVED BY THE CITY COUNCIL OF THE CITY OF VALDEZ, ALASKA, this 19th day of March, 2024.

City of Valdez, Alaska

_____
Sharon Scheidt, Mayor

ATTEST:

_____
Sheri L. Pierce, MMC, City Clerk

STATE OF ALASKA

STATEWIDE

CYBERSECURITY STRATEGIC

PLAN (SCSP)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM CYBERSECURITY PLANNING COMMITTEE **2**

CYBERSECURITY PLAN ELEMENTS **6**

ENHANCE PREPAREDNESS **9**

FUNDING & SERVICES **16**

ASSESS CAPABILITIES **16**

IMPLEMENTATION PLAN **17**

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT **19**

APPENDIX B: PROJECT SUMMARY WORKSHEET **23**

APPENDIX C: ENTITY METRICS **24**

APPENDIX D: ACRONYMS **26**

APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES **27**

APPENDIX F: KEY TERMS AND DEFINITIONS **29**

LETTER FROM CYBERSECURITY PLANNING COMMITTEE

Dear Cybersecurity Practitioners,

On behalf of the Alaska State and Local Cybersecurity Grant Program (SLCGP) Planning Committee I am pleased to introduce the 2023 Statewide Alaska Cybersecurity Strategic Plan. This plan reflects the State's continued dedication to enhancing cybersecurity and supporting the public entities within Alaska, as well as collaborating with our local partners.

The Cybersecurity Plan was developed through a collaborative effort of the State of Alaska (SOA) boroughs, cities, tribes, public education, and health institutions throughout the state. It incorporates best practices for managing cybersecurity risks and includes actionable and measurable goals and objectives focusing on the following priorities:

1. Enhance Cybersecurity Resilience and Interoperability
2. Foster a Cybersecurity Culture
3. Strengthen Cybersecurity Collaboration and Partnerships
4. Improve Cyber Incident Management and Response Capabilities

These goals and objectives are designed to help us navigate the ever-changing cybersecurity landscape and plan for new technologies. The Cybersecurity Plan aligns with the requirements of the U.S. Department of Homeland Security for the State and Local Cybersecurity Grant Program (SLCGP) and will serve as a reference point to help evaluate grants requested under that program. In addition, it is a powerful resource to provide practical guidance, coordination, and common understanding throughout the public sector in Alaska.

We recognize the importance of collaboration across disciplines and jurisdictions. Our plan emphasizes the need for partnership and information sharing with local governments, tribes, federal agencies, private sector, academic institutions, and non-profit organizations.

We are committed to achieving the goals outlined in the Cybersecurity Plan and to increase Alaska's cyber resilience. With the help of cybersecurity practitioners and engaged leaders, we can continue to improve our resilience and ensure the safety and security of our state's critical systems and information.

Thank you for your efforts to improve cybersecurity performance throughout the state. We look forward to continuing to work with you to achieve our cybersecurity objectives.

Sincerely,

DocuSigned by:

1DFC79A539D734CD...

Bill Smith
Chief Information Officer
State of Alaska | Department of Administration
Planning Committee Co-Chair

DocuSigned by:

F327D0318D0B47B...

Bryan J Fisher
State Authorized Agent
Planning Committee Co-Chair

INTRODUCTION

The State of Alaska Statewide Cybersecurity Strategic Plan (SCSP) is a key component to helping Alaska increase its cyber resilience. Representatives from across the spectrum of Alaska public sector agencies used existing plans, structures, and other relevant efforts to develop this comprehensive cybersecurity plan. Building upon existing structures and capabilities allows Alaska to provide governance and a framework to meet Alaska's critical cybersecurity needs while making the best use of available resources. Members of the planning committee consulted with local governments and associations of local governments and incorporated their feedback into this cybersecurity plan through a collaborative approach. The Department of Military and Veteran Affairs and the Office of the CIO in the Department of Administration partnered to form a Statewide Alaska Cybersecurity Strategic Plan Support Team. The support team established regular communication channels with local governments to gather feedback and input on the cybersecurity plan. This involved holding regular meetings to discuss cybersecurity challenges, share best practices, and gather feedback. This plan represents a baseline that will continue to improve and evolve over time, incorporating continuous input and responding to the ever-changing threat landscape. It is designed to focus on common principles that will help build a strong foundation across all levels of public agencies.

The SCSP support team recognizes the importance of involving these stakeholders in the cybersecurity planning process and ensured that their perspectives and insights were incorporated into the plan. By incorporating feedback from local jurisdictions, the State of Alaska meets requirements **SLCGP: e.2.A.ii.**

The Cybersecurity Plan is a two-year strategic planning document that contains the following components:

- **Vision and Mission**: The vision of the plan is to enhance Alaska's cybersecurity posture and resilience to mitigate cyber threats and vulnerabilities. The mission is to develop and implement a comprehensive cybersecurity strategy that involves all stakeholders and ensures the safety and security of Alaska's critical infrastructure and systems.
- **Organization, and Roles and Responsibilities:** This section describes the current roles and responsibilities for cybersecurity within the state, including any governance mechanisms in place. It also identifies the successes, challenges, and priorities for improvement. The plan outlines a strategy for the cybersecurity program and the organization structure that supports it. Additionally, the governance framework outlines authorities and requirements for the cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any state or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** The plan describes how feedback and input from local governments and associations were incorporated to reduce overall cybersecurity risk across Alaska. This was achieved through stakeholder engagement, meetings, and workshops, to ensure a holistic approach to developing the cybersecurity plan.
- **Cybersecurity Plan Elements:** This section outlines the technology and operations needed to maintain and enhance resilience across the cybersecurity landscape. The plan includes the 16 required elements outlined in the State and Local Cybersecurity

Improvement Act, including managing, monitoring, and tracking information systems, enhancing preparation and response to incidents, implementing continuous cybersecurity risk management practices, adopting best practices and methodologies, promoting the delivery of safe and trustworthy online services, ensuring continuity of operations, enhancing the cybersecurity workforce, and mitigating risks to critical infrastructure and key resources.

- **Funding:** The plan describes funding sources and allocations to build cybersecurity capabilities within the state, along with methods and strategies for funding sustainment and enhancement to meet long-term goals. This includes using cybersecurity grant funding to provide cost-effective and scalable cybersecurity services to local governments, including rural communities.
- **Implementation Plan:** The plan describes the state's approach to implementing, maintaining, and updating the Cybersecurity Plan to enable continued evolution and progress toward the identified goals. It includes a timeline for implementation and identifies the necessary resources needed to achieve the plan's objectives.
- **Metrics:** The plan describes how the state will measure the outputs and outcomes of the program across the state, including the use of key performance indicators (KPIs) to measure progress against the identified goals. This includes tracking the number of assessments, audits, exercises, and training sessions conducted, as well as the number of entities completing each component of the curriculum.

Vision and Mission

Alaska's vision and mission for improving cybersecurity practices statewide:

Vision:

Create a secure and resilient cybersecurity environment for the State of Alaska, where all state, local, and tribal governments work together seamlessly to protect against cybersecurity risks and threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

Mission:

Develop and implement a comprehensive cybersecurity plan for the State of Alaska that incorporates existing plans and feedback from local governments, promotes the adoption of best practices and methodologies, and ensures the continuity of operations in the event of a cybersecurity incident. The outcomes form this planning effort and implementation will include: assessment of the capabilities of the eligible entity relating to the actions described in the plan and identify and mitigate any gaps in the cybersecurity workforce, enhancement of the delivery of safe and trustworthy online services and work to establish strong partnerships to improve information sharing and collaboration. , and collaboratively striving to achieve measurable progress towards reducing cybersecurity risks and identifying, responding to, and recovering from

cybersecurity threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

Cybersecurity Program Goals and Objectives

State of Alaska Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. **Enhance Cybersecurity Resilience and Interoperability.** Encourage and support cybersecurity resilience by promoting the adoption of risk management programs that incorporate best practices and methodologies. Encourage alignment of information and operational technology cybersecurity objectives, and advocate for the establishment of an information and operational technology modernization cybersecurity review process.	1.1 Support and encourage a cybersecurity risk assessment of state and local government information systems to identify vulnerabilities and develop a risk management plan. Support the establishment of risk assessment protocols and provide guidance and resources to aid in the identification of potential cybersecurity risks and vulnerabilities. 1.2 Support and encourage the implementation of a continuous monitoring program to identify and mitigate cybersecurity risks and threats to information systems owned or operated by the state or local governments within Alaska. Promote the adoption of continuous monitoring practices and provide support to organizations and agencies in their efforts to identify and mitigate potential cybersecurity risks and threats.
2. **Foster a Cybersecurity Culture.** Encourage and support the fostering of a cybersecurity culture by promoting awareness and training programs for state employees, contractors, and local government personnel. Encourage the adoption of such programs and support the efforts of organizations and agencies in providing cybersecurity education and training to their employees and stakeholders.	2.1 Support and encourage the development and delivery of cybersecurity awareness and training programs to state employees, contractors, and local government personnel. Promote the adoption of such programs and provide resources and guidance to aid in the development and delivery of effective cybersecurity education and training. 2.2 Support and encourage the establishment of a cybersecurity awareness program to educate citizens on best practices and cybersecurity risks. Advocate for the adoption of awareness programs and provide resources and guidance to organizations and agencies in their efforts to educate citizens on cybersecurity risks and promote best practices.

Program Goal	Program Objectives
3. **Enhance Cybersecurity Collaboration and Partnerships.** Support and encourage the enhancement of Cybersecurity Collaboration and Partnerships by promoting the development of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and fostering cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations. Advocate for the establishment of information sharing protocols and encourage organizations and agencies to form partnerships and collaborations that promote effective cybersecurity practices and information sharing.	3.1 Support and encourage the development and implementation of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies. Advocate for the establishment of information sharing protocols and provide resources and guidance to organizations and agencies in their efforts to develop and implement effective information sharing programs. 3.2 Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations to develop and implement best practices.
4. **Improve Cybersecurity Incident Management and Response Capabilities.** Support and encourage the development and implementation of a cybersecurity incident response plan that outlines the roles, responsibilities, and procedures for responding to and recovering from cybersecurity incidents. Provide guidance and resources to aid in the establishment of incident response protocols and support organizations and agencies in their efforts to effectively respond to cybersecurity incidents.	3.3 Support and encourage the establishment of a cybersecurity incident response team with appropriate roles and responsibilities and promote the training and equipping of the team to respond to cybersecurity incidents. Provide resources and guidance to organizations and agencies in their efforts to establish incident response teams and ensure their readiness to respond to cybersecurity incidents. 3.4 Support and encourage the development and implementation of a cybersecurity incident management plan that outlines the procedures for responding to cybersecurity incidents and the roles and responsibilities of all stakeholders involved. Advocate for the adoption of incident management plans and provide support to organizations and agencies in their efforts to effectively respond to cybersecurity incidents.

CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

- State of Alaska Emergency Operations Plan (EOP) available at https://ready.alaska.gov/plans/
- State of Alaska 2023 -2025 Integrated Preparedness Plan (IPPW) available at https://ready.alaska.gov/Documents/Preparedness/Exercise/IPP%20SFY2023-2025.pdf
- Small Community Emergency Response Plan (SCERP), plan can be accessed by contacting the Alaska Division of Homeland Security and Emergency Management at mvaplanning@alaska.gov
- State of Alaska Hazard Mitigation Plan, available at https://ready.alaska.gov/Mitigation/SHMP

MANAGE, MONITOR, AND TRACK

The State of Alaska recognizes the critical importance of managing, monitoring, and tracking information systems, applications, and user accounts to effectively protect against cybersecurity risks and threats. To achieve this goal, the State will take – and encourage local governments to take – a comprehensive, integrated, and risk-based approach that incorporates the best practices and methodologies outlined in the Cybersecurity plan. Our strategic approach will focus on the following key areas.

Inventory Management

The State of Alaska encourages and supports the development of an inventory management program that includes all hardware and software used by the State, to include local government entities as feasible and decided locally. The inventory management program should incorporate prioritized risk to each item and should be reviewed and updated at least annually. This program will ensure that we have an accurate and up-to-date inventory of all information systems, applications, and user accounts, as well as any legacy systems that are no longer supported by the manufacturer. We encourage and support the development of policies and procedures for managing, monitoring, and tracking these systems to ensure that they are effectively protected against cybersecurity risks and threats.

Continuous Monitoring

The State of Alaska encourages and supports a continuous monitoring program that includes monitoring of activity, and behavior across all information systems, applications, and user accounts owned or operated by the State and encouraged for all local governments to implement and share. The program should leverage advanced technologies and tools to identify and mitigate cybersecurity risks and threats, including those that may target legacy systems. We also encourage and support the establishment of processes for responding to any alerts or incidents identified through the continuous monitoring program. The monitoring program should include identification of privileged accounts, key data and where it is stored and ensure it confidentiality, integrity, and availability.

Risk-Based Vulnerability Management

We encourage a risk-based vulnerability management program that includes regular vulnerability assessments and threat mitigation practices prioritized by the degree of risk to address cybersecurity risks and threats on all information systems, applications, and user accounts owned or operated by the state or local governments. This program should incorporate best practices and methodologies, to ensure that we are effectively managing, monitoring, and tracking vulnerabilities and threats.

Legacy System Management

We recognize that legacy systems that are no longer supported by the manufacturer are particularly vulnerable to cybersecurity threats. To address this vulnerability, we will encourage and support the implementation of a comprehensive legacy system management program that includes special focus on managing, monitoring, and tracking these systems to effectively protect, detect, respond to, and recover from cybersecurity incidents. This program should also include strategies for modernizing or replacing legacy systems where necessary.

While we understand that some eligible grant recipients may face constraints preventing them from replacing their legacy systems, we strongly encourage them to prioritize the implementation of compensating controls. Compensating controls serve as alternative measures to achieve cybersecurity objectives when traditional controls are not feasible or practical. By implementing these controls, entities

can mitigate the risks associated with legacy systems and reduce the likelihood and impact of cybersecurity incidents. We are committed to collaborating with such entities, assisting them in identifying and implementing compensating controls that are suitable for their specific needs and circumstances.

By adopting a comprehensive, integrated, and risk-based approach to managing, monitoring, and tracking information systems, applications, and user accounts, the State of Alaska will improve its cybersecurity resilience and interoperability over the next two years, and beyond. This approach will ensure that we are effectively protecting against cybersecurity risks and threats, including those that target legacy systems, and that we are able to detect, respond to, and recover from incidents in a timely and effective manner meet the requirement SLCGP: e.2.B.iv.

MONITOR, AUDIT, AND TRACK

The State of Alaska recognizes the importance of monitoring, auditing, and tracking network traffic and activity to enhance cybersecurity resilience across state and local government entities. While Alaska does not have a centralized security / information technology operation center (SOC / ITOC) to monitor, audit, and track network traffic and activity across all SLTTs currently, the state does support and encourage the following to monitor, audit, and track network traffic and activity:

- **Decentralized Monitoring:** SLTTS can be responsible for monitoring, auditing, and tracking their own network traffic and activity. This can be done using a combination of commercial and open-source tools and can be supplemented by training and information sharing initiatives to ensure that entities have the knowledge and skills necessary to monitor their networks effectively.

- **Partnerships with Managed Security Service Providers (MSSPs):** SLTTs can establish partnerships with MSSPs to monitor, audit, and track network traffic and activity on behalf of entities within their jurisdiction. This can be done through contracts with the MSSPs, who can provide centralized monitoring and reporting capabilities.

- **Cloud-based Security Services:** SLTTs can leverage cloud-based security services to monitor, audit, and track network traffic and activity. This can be done through contracts with cloud service providers, who can provide centralized monitoring and reporting capabilities.

- **Collaborative Monitoring:** SLTTs can establish a collaborative monitoring program that brings together entities within their jurisdiction to share monitoring data and collaborate on threat identification and response. This can be done using a shared platform that enables entities to share data and collaborate on threat identification and response.

  SLTTs are encouraged to leverage established partnerships with agencies such as CISA, MS-ISAC, and/or vendor network monitoring, auditing, and tracking services to enhance their capabilities for monitoring, auditing, and tracking network traffic and activity. By doing so, state and local government can leverage best practices and expertise across the cybersecurity community to enhance Alaska's overall cybersecurity posture. The State of Alaska has partnered with a variety of organizations to bolster its cybersecurity measures. One such partnership is with the Alaska Federation of Natives, which launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills. The state has also partnered with Arctic Slope Regional Corporation and the University of Alaska to establish the Alaska Cybersecurity Center, which offers

training and research opportunities to students and professionals. Additionally, the state has worked with the Department of Homeland Security to conduct cybersecurity risk assessments and develop response plans.

These partnerships demonstrate the State of Alaska's commitment to staying ahead of cyber threats and ensuring that its citizens, businesses, and infrastructure are protected. By collaborating with various organizations, the state can leverage their expertise and resources to create a more secure cyber landscape.

- Network Security: SLTTs can establish a comprehensive network security program that includes all information systems, applications, and user accounts owned or operated by the state or local government entities within the jurisdiction of the state. This program should incorporate best practices and methodologies to ensure that the SLTTs are effectively monitoring, auditing, and tracking vulnerabilities and threats. By doing so, the SLTTs will enhance their cybersecurity resilience and interoperability by ensuring that we are effectively securing our network infrastructure.

The State of Alaska and the SLCGP planning committee will identify and assist with coordinating activities between local government entities and federal partners to enhance network monitoring, auditing, and tracking of network traffic and activity. By leveraging partnerships, cloud-based services, collaborative monitoring programs, and cybersecurity services, the state aims to ensure effective cybersecurity resilience, information sharing, and interoperability across all levels of government. This commitment aligns with our goal to stay ahead of cyber threats and protect the state's citizens, businesses, and infrastructure, and enhance their overall cybersecurity resilience meeting the requirement of SLCGP: e.2.B.iv.

ENHANCE PREPAREDNESS

The State of Alaska will collaborate with relevant agencies and stakeholders to develop and implement a comprehensive cybersecurity preparedness plan that includes all levels of government within the state. The plan will be based on Risk Management Best Practices and Frameworks and will identify and prioritize key resources that are vital to the state's economy, public health, and safety.

We will work with relevant state, local and federal agencies to provide training and exercise support to SLTT organizations to enhance their cybersecurity preparedness. The State of Alaska recommends these activities include tabletop exercises, functional exercises, and full-scale exercises to test and evaluate the state's cybersecurity response capabilities.

Additionally, we will expand ongoing training programs to enhance the knowledge and skills of personnel within the community to address cybersecurity risks and threats. The recommended topics include cybersecurity hygiene training, awareness campaigns, and training on the latest cybersecurity technologies and best practices.

To enhance our response capabilities, we will develop and implement incident response plans and procedures to address cybersecurity incidents promptly and effectively. We will also ensure that our response plans align with the National Incident Management System (NIMS) and the National Response Framework (NRF).

Through these efforts, the State of Alaska will enhance its preparation, response, and resiliency against cybersecurity risks and threats, and promote and support that for SLTTs. As we achieve our program objectives, we will report our progress and outcomes to relevant stakeholders and adjust our strategies as necessary.

Assessment and Mitigation

The State of Alaska's strategic approach to implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk will focus on improving the state's ability to identify and mitigate cybersecurity threats and vulnerabilities on information systems, applications, and user accounts across state and local governments.

To achieve this, the state will encourage, support, and collaborate with local entities to develop comprehensive cybersecurity risk assessments to be performed annually, including identifying potential vulnerabilities and prioritizing mitigation efforts based on the level of risk. The State will also encourage and support the development and implementation of policies and procedures for vulnerability management, including timely application of security patches and updates, regular vulnerability scans, and penetration testing.

The State of Alaska acknowledges the significance of identifying and mitigating cybersecurity threats and vulnerabilities to uphold the ongoing protection of critical information systems, applications, and user accounts. As part of its commitment, the State of Alaska will require, through the grant process, grantees conduct a self-assessment and engage in ongoing follow-ups. This collaborative effort between state and local government entities will establish a continuous process of cybersecurity vulnerability assessments and threat mitigation practices, prioritized based on the degree of risk.

To ensure that local entities have access to the necessary tools and resources, the State will expand ongoing training, cyber incident exercise, and cybersecurity information sharing. By regularly assessing and mitigating cybersecurity threats and vulnerabilities, the State of Alaska will improve the overall cybersecurity posture of state and local government entities and meet the requirement SLCGP: e.2.B.iv.

Best Practices and Methodologies

The State of Alaska recognizes the importance of adopting and using best practices and methodologies to enhance cybersecurity. To improve the overall security posture of SLTT organizations, the following cybersecurity best practices will be encouraged, and eligible for available grant funding, to be implemented within a reasonable timeline according to the prioritization that emerges from the self-assessment:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Identify and implement compensating controls to mitigate threats to unsupported software and hardware
- Prohibit use of known/fixed/default passwords and credentials
- Ensure the ability to reconstitute systems (backups)
- Migrate to the .gov internet domain
- Implement network boundary filtering capabilities where practicable (e.g., DNS, URL, Email)
- Implement [cyber]security awareness training program.

- Implement authentication and privileged account access in alignment with best practices and standards on an annual basis.
- Implement a Patch Management Solution

These best practices will be incorporated statewide and individual projects that assist SLTT entities adopting these best practices will be prioritized.

NIST Principles

In addition to the above best practices, the State of Alaska will adopt recognized frameworks such as NIST Cybersecurity Framework (CSF) or equivalent frameworks to significantly improve its ability to meet cybersecurity requirements. The State of Alaska will work to implement NIST CSF or an equivalent framework as the foundation for its Cybersecurity Program and work towards its widespread adoption among state and local entities.

Supply Chain Risk Management

Supply Chain Risk Management is a critical aspect of cybersecurity, and the State of Alaska will adopt cyber supply chain risk management (C-SCRM) best practices identified by NIST. The state will identify, prioritize, and assess information technology suppliers, vendors, and service providers – including to work with and through local partners - to understand the related and/or cascading risks to the state and local supply chain.

Tools and Tactics

To continuously improve cybersecurity best practices, the State of Alaska will engage with MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics. The State encourages SLTTs to participate in government and cybersecurity conferences and liaise with cybersecurity professionals from federal, state, and private entities to share indicators of compromise, best practices, and threat intelligence. Partnerships with affiliated organizations will enhance the State's ability to share opportunities and information.

Safe Online Services

The State of Alaska is committed to promoting the delivery of safe, recognizable, and trustworthy online services. As part of this effort, the state is encouraging the use of the .gov internet domain for all state agencies and local entities that are eligible for the domain.

To support the adoption of the .gov domain, the state is providing technical assistance and resources to eligible entities. This includes guidance on how to obtain a .gov domain, as well as assistance with domain registration and implementation. Additionally, the state is promoting the use of cybersecurity tools, such as external vulnerability scanning, automated vulnerability monitoring, scanning, and reporting to ensure that online services are safe and secure.

The state is also committed to ongoing education and awareness efforts to promote safe online practices among employees and the public. This includes regular cybersecurity training and awareness campaigns, as well as public outreach initiatives to raise awareness about online risks and best practices for staying safe online.

By promoting the use of the .gov domain and providing resources and support for safe online services, the State of Alaska is demonstrating its commitment to enhancing cybersecurity and ensuring the delivery of safe and trustworthy online services.

Continuity of Operations

Continuity of Operations (COOP) planning is essential to ensure the delivery of critical services and operations in the event of a cyber incident. The State of Alaska will establish a comprehensive COOP program to ensure the continuity of critical services and operations during and after a cyber incident. This program will be developed in coordination with the Alaska Division of Homeland Security and Emergency Management and will include partnerships with local and tribal governments.

The State of Alaska will provide resources to support COOP planning and emergency response efforts. The State will also promote ongoing training and exercises to enhance COOP preparedness and response capabilities.

For this two-year Plan, the State of Alaska will prioritize the development of viable, comprehensive COOP plans and business continuity programs for state agencies, local governments, and tribal entities. The State will collaborate with partners to expand ongoing training, cyber incident exercise, and cybersecurity information sharing, which will support local entities' COOP planning efforts.

The State will also establish performance measures to track the maturity of COOP planning efforts and incident response preparedness. The State of Alaska is committed to ensuring continuity of operations in the face of cyber incidents and demonstrates that the plan meets requirement SLCGP: e.2.B.vii.

Workforce

The State of Alaska is committed to using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as improving personnel's knowledge, skills, and abilities to address cybersecurity risks and threats.

To support this initiative, the State of Alaska will work to build alliances with employers, educational institutions, and public and private partners to develop training and educational pathways to provide the needed skilled workers in the cybersecurity field.

Initiatives will focus on developing internships and apprenticeships, promoting cybersecurity education in K-12 and higher education, and utilizing state-supported internship programs.

The State of Alaska will also provide ongoing training to personnel at all levels in good cyber hygiene and best cybersecurity practices. This will include promoting the adoption of the NICE Framework in state and local hiring practices and encouraging interested individuals to further develop their cybersecurity skills through internships and educational opportunities.

The State will continue to monitor the its cybersecurity workforce and promote the adoption of best practices and the NICE Framework to ensure the State of Alaska has a skilled and effective cybersecurity workforce, meeting requirement SLCGP: e.2.B.viii.

Continuity of Communications and Data Networks

The State of Alaska recognizes the critical need for cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks. To address this need, the State of Alaska will ensure that all entities have access to a comprehensive and regularly

updated Incident Response Plan that provides instructions for communication during an incident and how to handle situations where the secure and preferred communication method is unavailable.

The State of Alaska will ensure that all entities are trained in the use of these communication and data network systems and will conduct regular exercises to test their effectiveness in maintaining continuity of operations. The State of Alaska will also establish procedures for the use of Traffic Light Protocol (TLP) when sharing incident information to ensure that sensitive information is only shared with appropriate audiences.

Through these efforts, the State of Alaska will ensure cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks, meeting requirement SLCGP: e.2.B.ix.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

The State of Alaska Division of Homeland Security and Emergency Management (DHSEM) conducts a federally required Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) every three years. The State recognizes the importance of assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources, such as power and telecommunications, that may impact the performance of information systems within its purview. To accomplish this goal, the state will conduct regular assessments of its capabilities across relevant mission areas, including Prevention, Protection, Mitigation, Response, and Recovery.

Alaska will encourage and support the use of established frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or equivalent, to guide its assessment and mitigation efforts. These assessments target federal and state funding to mitigate cybersecurity risks and threats to critical infrastructure and key resources.

The state will work closely with its partners, including local jurisdictions and private sector organizations, to identify and prioritize critical infrastructure and key resources and develop strategies to enhance their cybersecurity posture. The state will share and promote the adoption of best practices and cybersecurity frameworks, such as the NIST Cybersecurity Framework, to ensure that critical infrastructure and key resources are protected to the greatest degree possible.

Alaska recognizes that assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources is an ongoing process that requires continuous monitoring and improvement. The state will regularly review and update its strategies and plans to ensure that they remain effective and responsive to the evolving threat landscape. These efforts demonstrate that the state is committed to meeting requirement SLCGP: e.2.B.x.

Cyber Threat Indicator Information Sharing

The State of Alaska is committed to enhancing its capacity and capabilities to share cyber threat indicators and related information with relevant stakeholders. To achieve this goal, we will leverage CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems, and other applicable systems and processes.

Additionally, we will encourage all entities to subscribe to and participate in the MS-ISAC Real-Time Indicator Feeds to stay up to date on emerging threats and vulnerabilities. We will also promote the adoption of CISA's free cybersecurity services to local entities through outreach efforts and state and federal partnerships.

As part of our commitment to information-sharing, we will maintain active collaborations with our federal, state, local, tribal (SLTT) partners, as well as organizations like the Alaska Municipal League (AML), to collectively identify and address cybersecurity threats and vulnerabilities. By leveraging these partnerships, we aim to enhance our ability to identify and mitigate potential risks to our critical infrastructure and key resources, thereby ensuring the uninterrupted continuity of our operations even in the face of a cyber incident. This comprehensive plan aligns with and fulfills the requirement SLCGP: e.2.B.xii.

Department Agreements

The State of Alaska is committed to sharing cyber threat indicators and related information with all SLTTs, including expanding information sharing agreements with CISA. Alaska will expand information sharing by working with partners by developing options for centralizing communication and information sharing to share cyber threat information products with federal, and SLTT partners. The SLCGP committee will continue to work towards expanding and evolving the sharing of cyber threat indicators, incidents after action reports, and other related information with CISA and MS-ISAC. As part of Alaska's cybersecurity plan, we will focus on improving and enhancing cybersecurity intelligence and information sharing across all levels of government, including local, regional, state, and federal organizations. Through this plan, we will initiate projects to achieve this goal and expand our capability to share cyber threat indicator information with DHS, meeting requirement SLCGP: e.2.B.xi.I-II.

Leverage CISA Services

The State of Alaska recognizes the importance of leveraging the cybersecurity services offered by CISA to enhance our cybersecurity posture. Alaska currently participates in several CISA programs, including the Automated Indicator Sharing (AIS) and the Cyber Hygiene program.

The Alaska Division of Homeland Security and Emergency Management (DHSEM) will continue to collaborate with CISA to identify opportunities to expand our participation in these programs and explore additional cybersecurity services offered by CISA that could benefit our state.

DHSEM will also work to increase awareness of the benefits of these services among state and local entities and promote adoption of CISA's cybersecurity best practices and guidelines. The State encourages CISA to ensure adequate timeliness and responsiveness to needs especially of SLTTs, including to provide technical assistance as they implement local planning efforts.

Through these efforts, Alaska aims to strengthen our cybersecurity capabilities and meet the requirements of SLCGP: e.2.B.xii.

Information Technology and Operational Technology Modernization Review

The State of Alaska is committed to ensuring alignment between information technology (IT) and operational technology (OT) cybersecurity objectives. As part of this Statewide Alaska Cybersecurity Strategic Plan, we will encourage and support a modernization review process to identify and mitigate cybersecurity risks and threats to IT and OT systems.

The State encourages and supports regular assessments of IT and OT systems to ensure they are properly secured and updated. We will prioritize the implementation of security controls and risk management strategies to address any vulnerabilities identified during these assessments.

To ensure effective alignment between IT and OT cybersecurity objectives, we will encourage and support the creation of a cross-functional team comprising IT and OT professionals from SLTTs who will work collaboratively to identify and mitigate cybersecurity risks and threats. This team will be responsible for

evaluating new technologies and solutions to ensure they are secure and compatible with both IT and OT systems.

We will continue to establish partnerships with industry experts and vendors who specialize in OT cybersecurity to gain valuable insights and expertise in securing critical infrastructure and key resources. These partnerships will help us identify emerging threats and vulnerabilities, as well as best practices for securing IT and OT systems.

Through these efforts, we will ensure that our IT and OT systems are secure and resilient, and that we can effectively respond to and mitigate cybersecurity risks and threats to our critical infrastructure and key resources.

Cybersecurity Risk and Threat Strategies

The SLCGP Committee of the State of Alaska will develop and coordinate strategies to address cybersecurity risks and threats in collaboration with other organizations. This will include consulting with local governments and associations of local governments, neighboring entities, and Tribal governments, or members of an ISAC; and other states. We will establish a process to ensure effective communication and collaboration with relevant entities and organizations. We will participate in the activities of organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) to enhance information sharing and collaboration with other states.

Our approach will involve regular coordination and information sharing with neighboring entities, , and Tribal governments to ensure that we have a comprehensive understanding of cybersecurity risks and threats in our region. We will work with these entities to develop coordinated response plans and strategies to address cybersecurity incidents that affect our jurisdictions.

In addition, we will collaborate with federal agencies such as the Department of Homeland Security and the Federal Bureau of Investigation to enhance our cybersecurity capabilities and ensure effective incident response. The State of Alaska is committed to a proactive and collaborative approach to cybersecurity risk and threat strategies, meeting requirement SLCGP: e.2.B.xiv.

Rural Communities

The State of Alaska recognizes the importance of ensuring that rural communities have adequate access to and can participate in cybersecurity services and activities. As a geographically expansive state, with many rural and remote communities, the state government is committed to providing cybersecurity services and resources to all Alaska public and local entities, regardless of their location or socioeconomic status.

To achieve this goal, the state government will work closely with local governments, associations of local governments, and tribal governments to identify and address any barriers to access that may exist in rural communities. This will involve consultation with these communities to understand their unique needs and challenges related to cybersecurity.

The state government will also help public sector entities explore the use of technology to provide cybersecurity services and resources to rural communities. This may include the use of virtual training and educational materials, as well as remote access to cybersecurity experts and support services.

In addition, the state government will promote public-private partnerships that can help to address the cybersecurity needs of rural communities. This may involve working with local businesses, non-profits, and other organizations to provide cybersecurity training and support to individuals and organizations in rural areas.

Overall, the State of Alaska is committed to ensuring that all Alaska entities, regardless of their location or background, have access to the cybersecurity services and resources they need to protect themselves and their communities from cyber threats.

FUNDING & SERVICES

The State of Alaska plans to utilize grant funding to support its comprehensive cybersecurity plan, including initiatives to improve the cybersecurity practices of state agencies and local entities. The state will distribute funds, items, services, capabilities, or activities to local governments, including plans to distribute at least 25% of cybersecurity grant funding received to rural areas.

In the first year of the program, the State of Alaska will focus on providing cost-effective and scalable cybersecurity services to local governments, including rural communities. These services will include assessments, audits, continuity planning, response planning, exercises, and skill enhancement for local entities. The state will work directly and collaborate with relevant agencies and partners to ensure a comprehensive and multi-faceted approach.

The State of Alaska will also work to expand and evolve cybersecurity practices across state agencies through improving vulnerability management and penetration testing and creating metrics and reports to prioritize remediation action. The state will use NIST 800-53 as a framework for implementing these initiatives.

Distribution to Local Governments

The State of Alaska aims to support local governments through implementing its comprehensive cybersecurity plan and by providing resources that enable delivery of the plan's objectives. These details will be listed in a table found in Appendix B: Project Summary Worksheet. To ensure the successful implementation of the cybersecurity plan, the state will distribute funds, items, services, capabilities, or activities to local governments. Additionally, the state plans to allocate at least 25% of the cybersecurity grant funding received specifically to rural areas.

ASSESS CAPABILITIES

The State of Alaska will adopt a strategic approach to assess the capabilities of entities applying for funding through the grant program for the various cybersecurity plan elements. This approach aims to comprehensively evaluate the cybersecurity capabilities of each entity, specifically addressing the requirements outlined in Appendix A: Cybersecurity Plan Capabilities Assessment. The assessment of Alaska's cybersecurity capabilities will be conducted at different levels, namely Foundational, Fundamental, Intermediate, and Advanced.

To assess these capabilities, the State of Alaska will leverage the NIST Cybersecurity Framework and the NICE Workforce Framework for Cybersecurity. Furthermore, a gap analysis will be conducted to identify areas that require improvement and enhancement in terms of cybersecurity capabilities. The State will support and encourage SLTTs to perform their own gap analysis that can be funded through the grant program.

Based on the assessment outcomes, Alaska will identify areas that necessitate increased capabilities and will develop action plans to address those gaps. Clear assignment of responsibilities to relevant parties and target completion dates will be established for each action plan.

In addition, periodic assessments will be conducted to ensure the continuous effectiveness of Alaska's cybersecurity capabilities in addressing emerging cyber threats and risks. These assessments will follow a regular schedule and involve all relevant stakeholders.

Overall, Alaska remains dedicated to the ongoing enhancement of its cybersecurity capabilities, ensuring effective protection of information systems and critical infrastructure against cyber threats and risks.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

The Department of Administration, under the State of Alaska, takes the lead in managing the executive branch cybersecurity program. Specifically, it oversees the Office of Information Technology (OIT), which is responsible for safeguarding and managing the IT infrastructure of the state's executive branch. The OIT ensures the implementation of cybersecurity policies and standards, and its primary focus is on securing the executive branch's IT systems and infrastructure. The SLCGP Committee, consisting of representatives from various state agencies and levels of government, is responsible for developing and implementing the Statewide Alaska Cybersecurity Strategic Plan. The Committee will coordinate with local governments and associations, neighboring entities, Tribal governments, and ISACs to ensure effective implementation of the Plan.

The following roles and responsibilities have been defined for the implementation of the Statewide Alaska Cybersecurity Strategic Plan:

- The Department of Administration will serve as the lead agency for the cybersecurity program and oversee the implementation of the Plan.
- The OIT will manage and secure the state's IT infrastructure, oversee compliance with cybersecurity policies and standards, and ensure the implementation of the Plan.

The State of Alaska, through its Emergency Management and grant administration, will play a vital role in the development, implementation, and coordination of the comprehensive cybersecurity plan. The SLCGP (State and Local Cyber Grant Program) Committee will take the lead in developing and implementing the plan, ensuring effective coordination with other organizations involved in cybersecurity efforts. Furthermore, the committee will oversee the overall implementation of the plan, working closely with the State of Alaska Emergency Management and grant administration to ensure its successful execution. Each goal and objective in the Plan has a timeline with a target completion date and one or more owners responsible for overseeing and coordinating its completion. Accomplishing the goals and objectives will require support and cooperation from various individuals, groups, or agencies. Regular governance body meetings will include formal agenda items for reviewing the progress of the Plan's implementation.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

The implementation of this comprehensive cybersecurity plan will require collaboration, resources, and investments across the State of Alaska. The resources needed to execute this plan include funding, personnel, and technology.

Funding will be needed to support the implementation of cybersecurity tools and technologies, as well as to develop and execute training and awareness programs. Personnel will be required to support the implementation of the cybersecurity plan, including cybersecurity professionals to conduct risk

assessments, manage cybersecurity tools, and provide training to personnel. Technology investments will be necessary to enhance the security posture of the state's information systems and networks.

The timeline for implementing the cybersecurity plan is as follows, for the State, with corresponding support for local governments and Tribes to align their efforts to this schedule:

- Year 1: Conduct a comprehensive risk assessment of the state's information systems and networks, identify critical infrastructure, and key resources, and develop a cybersecurity training and awareness program for state personnel.
- Year 2: Implement additional cybersecurity tools and technologies, including endpoint protections, data loss prevention, and multifactor authentication. Continue to expand the use of the .gov domain and cybersecurity tools to boroughs and cities. Grantees can apply for funding to implement these tools.
- Year 3: Develop and implement a continuity of operations plan for cybersecurity incidents and conduct regular exercises to test the plan. Expand ongoing training, cyber incident exercises, and cybersecurity information sharing to support local entities.
- Year 4: Focus on workforce development, using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the state's cybersecurity workforce. Continue to leverage CISA services and expand information sharing agreements with local governments. Conduct a review of information technology and operational technology modernization to ensure alignment between cybersecurity objectives.
- Year 5: Develop and coordinate strategies to address cybersecurity risks and threats with other organizations, including consultation with local governments, neighboring entities, territories, and tribal governments. Ensure rural communities have adequate access to and can participate in cybersecurity services and activities.

These timelines are subject to change based on the availability of resources and other factors that may impact the state's ability to implement this comprehensive cybersecurity plan. The State of Alaska will regularly review and update this plan to ensure its effectiveness and relevance to the current cybersecurity landscape.

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY PLANNING COMMITTEE				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts	State agencies and some local jurisdictions currently manage, monitor, and track varying levels of information systems, applications, and user accounts	Foundational		
2. Monitor, audit, and track network traffic and activity	State agencies and some local jurisdictions currently monitor, audit, and track network traffic and activity	Foundational		
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	State agencies and some local jurisdictions engage in practices to enhance preparation, response, and resiliency	Foundational	1	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	State agencies and some local jurisdictions engage in regular cybersecurity assessments and risk	Foundational	2	

	management activities			
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	State agencies and some local jurisdictions implement the best practices listed in Plan Element 5	Foundational		
a. Implement multi-factor authentication	State agencies and some local jurisdictions implement MFA	Foundational		
b. Implement enhanced logging	State agencies and some local jurisdictions implement enhanced logging	Foundational		
c. Data encryption for data at rest and in transit	State agencies and some local jurisdictions utilize encryption for data at rest and in transit	Foundational		
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	State agencies and some local jurisdictions exercise life cycle management practices to end use of unsupported/end of life software and hardware	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	State agencies and some local jurisdictions prohibit use of known/fixed/default password and credentials	Foundational		

f. Ensure the ability to reconstitute systems (backups)	State agencies and some local jurisdictions ensure the ability to reconstitute critical systems	Foundational		
g. Migration to the .gov internet domain	State agencies and some local jurisdictions have or plan to migrate to .gov	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	State agencies and some local jurisdictions promote the delivery of safe, recognizable and trustworthy online services	Foundational		
7. Ensure continuity of operations including by conducting exercises	State agencies and some local jurisdictions conduct exercises	Foundational		
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	State agencies and some local jurisdictions identify and mitigate any gaps in the cybersecurity workforces	Foundational		
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	State agencies and some local jurisdictions ensure continuity of communications and data networks	Foundational		
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the	State agencies and some local jurisdictions assess and mitigate cybersecurity risks	Foundational	2	

performance of information systems within the jurisdiction of the eligible entity	and threats to critical infrastructure			
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	State agencies and some local jurisdictions enhance capabilities to share cyber threat indicators and information	Foundational		
12. Leverage cybersecurity services offered by the Department	State agencies and some local jurisdictions leverage cybersecurity services offered by the Department	Foundational		
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	State agencies and some local jurisdictions implement modernization cybersecurity review process	Foundational		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	State agencies and some local jurisdictions develop and coordinate strategies to address cybersecurity strategies and risks	Foundational		
15. Ensure rural communities have adequate access to, and participation in plan activities	State agencies and some local rural jurisdictions have adequate access to and participation in plan activities	Foundational		
16. Distribute funds, items, services, capabilities, or activities to local governments	State agencies are prepared to distribute grant funds and some services appropriately	Foundational	1	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

1. Rank	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
1	Statewide Cybersecurity Plan Refinement	Additional planning by Cybersecurity Planning Committee to refine the cybersecurity plan submission for FY2023	1, 2, 3, 4, 5, 6, 10, 12, 13, 14, 15, 16	$20K (TBD)	Ongoing	High	Plan
2	Direct pass-through funds to eligible local government entities based on strength of application, demonstrated need, rural designation, and evidence of ability to sustain investment	Applications will be prioritized based on following identified cybersecurity components: - Conduct vulnerability assessments - Implement multi-factor authentication - Implement enhanced logging - Data encryption for data at rest and in transit - End use of unsupported / end of life software and hardware that are accessible from the internet - Prohibit use of known/fixed/default passwords and credentials -Ensure ability to reconstitute systems (backups)	1, 2, 3, 4, 5, 6, 8, 10, 12, 13, 14, 15, 16	$XXM (TBD)	Future	High	Equip

APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics		
Cybersecurity Plan Metrics		
Goal	**Step**	**Key Performance Indicator**
1. Enhance Cybersecurity Resilience and Interoperability by developing and implementing a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies.	• Develop a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies. • Develop and implement a security awareness training program	• Number of cybersecurity risk assessments conducted annually. • Percentage of vulnerabilities remediated within a defined timeframe. • Compliance with relevant cybersecurity regulations and standards
2. Foster a Cybersecurity Culture by developing and delivering cybersecurity awareness and training programs to state employees, contractors, and local government personnel.	• Develop and deliver cybersecurity awareness and training programs to state employees, contractors, and local government personnel. • Develop and implement a security awareness campaign to increase awareness and promote best practices	• Number of training sessions conducted. • Percentage of employees completing the training • Number of reported security incidents related to employee behavior

Cybersecurity Plan Metrics		
Goal	**Step**	**Key Performance Indicator**
3. Enhance Cybersecurity Collaboration and Partnerships by developing and implementing a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations.	• Develop and implement a cybersecurity information sharing program with local governments, neighboring states, and federal agencies. • Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations	• Number of cybersecurity risk assessments conducted annually. • Percentage of vulnerabilities remediated within a defined timeframe. • Compliance with relevant cybersecurity regulations and standards
4. Improve Cyber Incident Management and Response Capabilities by developing and implementing a cybersecurity incident management plan that is tested and updated on a regular basis and establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents.	• Develop and implement a cybersecurity incident management plan that is tested and updated on a regular basis. • Establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents. • Conduct regular cybersecurity incident response exercises and drills	• Number of cybersecurity incident response exercises conducted annually. • Percentage of incidents handled within defined timeframes. • Effectiveness of incident response team in mitigating the impact of cybersecurity incidents.

APPENDIX D: ACRONYMS

Acronym	Definition
ISAC	Information Sharing and Analysis Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
SLCGP	State and Local Cybersecurity Grant Program
IT	Information Technology
SOC	Security Operations Center
ITOC	Information Technology Operations Center
MSSP	Managed Security Service Provider
CISA	Cybersecurity and Infrastructure Security Agency
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
C-SCRM	Cyber Supply Chain Risk Management
COOP	Continuity of Operations
DHSEM	Division of Homeland Security and Emergency Management
THIRA	Threat and Hazard Identification and Risk Assessment
SPR	Security and Privacy Requirements
CIMS	Cyber Incident Management System
TLP	Traffic Light Protocol
CISCP	Certified Information Systems Cybersecurity Professional
AIS	Automated Information System
SLTT	State, Local, Tribal, and Territorial

APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES

All recipients and subrecipients of the Statewide Alaska Cybersecurity Grant Program (SLCGP) are required to participate in the following free services provided by the Cybersecurity and Infrastructure Security Agency (CISA). Please note that participation in these services is not mandatory for grant submission and approval but is a post-award requirement.

REQUIRED SERVICES AND MEMBERSHIPS

Cyber Hygiene Services:

- **Web Application Scanning:** A service that assesses the health of publicly accessible web applications, identifies vulnerabilities, and recommends security enhancements.
- **Vulnerability Scanning:** Continuous scanning of public, static IPs for accessible services and vulnerabilities, providing weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP." In the body of your email, mention that you are requesting these services as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR):

The NCSR is an annual self-assessment that measures the cybersecurity programs' gaps and capabilities of state, local, and tribal (SLT) entities. It is based on the National Institute of Standards and Technology Cybersecurity Framework and sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Entities and subrecipients should complete the NCSR annually.

For more information, visit the Nationwide Cybersecurity Review (NCSR) website (cisecurity.org).

ENCOURAGED SERVICES, MEMBERSHIPS, AND RESOURCES

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):

Recipients and subrecipients are strongly encouraged to become members of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC: DHS-designated cybersecurity ISAC for SLT governments, providing services and information sharing to enhance their cybersecurity capabilities.

The EI-ISAC: Focuses on election infrastructure cybersecurity, offering cyber defense tools, threat intelligence products, incident response and forensics, cybersecurity awareness, and training.

To register, please visit the MS-ISAC registration page or the EI-ISAC registration page. For more information, visit MS-ISAC (cisecurity.org) and Election Infrastructure Security (cisa.gov).

CISA Recommended Resources, Assessments, and Memberships (not mandatory):

The following resources, assessments, and memberships are recommended by CISA:

- Cyber Resource Hub
- Ransomware Guide (Sept. 2020)
- Ransomware Readiness Assessment (RRA)
- Cyber Security Evaluation Tool (CSET)
- Malicious Domain Blocking and Reporting
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- CISA Services Catalog
- Free Public and Private Sector Cybersecurity Tools and Services

For reporting a cybersecurity incident, visit CISA Central at us-cert.gov/report. For additional CISA services, refer to the CISA Services Catalog. Information on memberships can be found at the Information Sharing and Analysis Organization Standards Organization.

Note: The inclusion of optional resources and memberships in this appendix does not imply mandatory participation but is provided for informational purposes and to support the enhancement of cybersecurity capabilities.

APPENDIX F: KEY TERMS AND DEFINITIONS

Alaska Cybersecurity Center: An organization established in partnership with the Alaska Federation of Natives and the University of Alaska to provide training and research opportunities in cybersecurity.

Alaska Federation of Natives: A partner organization that launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills.

Alaska Native Cybersecurity Enhancement Project: A collaborative initiative aimed at providing cybersecurity training to Alaska Natives.

Automated Indicator Sharing (AIS): A capability provided by the Cybersecurity and Infrastructure Security Agency (CISA) that allows for the automated exchange of cyber threat indicators.

Cloud-based Security Services: Security services and tools offered by cloud service providers (CSPs) to protect and monitor network infrastructure and data stored in cloud environments.

Collaborative Monitoring: A cooperative approach where multiple entities within a jurisdiction share resources, data, and expertise to collectively monitor and respond to cybersecurity threats.

Continuity of Operations (COOP) Planning: Efforts to ensure the continuity of critical services and operations in the event of a cybersecurity incident.

Continuity of Operations Plan (COOP): A plan outlining actions and procedures to be taken during and after a cybersecurity incident to ensure the continuity of critical operations.

Cross-Functional Team: A team comprising professionals from different disciplines or areas of expertise working together to achieve a common cybersecurity goal.

Cyber Incident Exercise: Simulated exercises designed to test the response and resilience of entities in handling cybersecurity incidents.

Cyber Information Sharing and Collaboration Program (CISCP): A program operated by the Cybersecurity and Infrastructure Security Agency (CISA) that facilitates information sharing and collaboration among cybersecurity stakeholders.

Cybersecurity Services: Services provided by specialized organizations or agencies to support the prevention, detection, response, and recovery from cybersecurity incidents.

Data Encryption: The process of converting data into a coded form to prevent unauthorized access, ensuring its confidentiality and integrity.

Data Loss Prevention (DLP): Measures and technologies implemented to prevent the unauthorized disclosure or loss of sensitive data.

Endpoint Protections: Security measures and tools implemented on endpoints (e.g., computers, laptops, mobile devices) to protect against cyber threats.

Funding Prioritization: The allocation of resources and funding based on prioritized cybersecurity risks and threats.

Gap Analysis: The process of identifying gaps or deficiencies in cybersecurity capabilities and developing plans to address them.

Governance Body: A formal body responsible for overseeing the implementation and progress of the cybersecurity plan.

Information Sharing: The process of exchanging relevant and actionable information between organizations or entities to enhance situational awareness, threat detection, and incident response capabilities.

Information Sharing Agreements: Formal agreements established to facilitate the sharing of cyber threat indicators and related information with local governments and other stakeholders.

Local Government: The governing body responsible for the administration and governance of specific local jurisdictions within a state, such as counties, cities, towns, or municipalities.

Managed Security Service Providers (MSSPs): Companies or organizations that offer outsourced cybersecurity services to assist in monitoring, managing, and enhancing an organization's security posture.

Mitigation: Actions taken to reduce the impact of cybersecurity incidents and vulnerabilities.

Modernization Review Process: A systematic assessment of IT and OT systems to identify and mitigate cybersecurity risks and threats.

Monitoring: The process of observing and collecting data or information to track the performance, behavior, or status of a system, network, or activity.

Multi-State Information Sharing and Analysis Center (MS-ISAC): An organization that facilitates the sharing of cyber threat information and collaboration among states.

Multifactor Authentication: A security mechanism that requires the use of multiple factors (e.g., password, biometric, token) for user authentication.

National Initiative for Cybersecurity Education (NICE) Workforce Framework: A framework used to categorize and describe cybersecurity work roles and required competencies.

Network Activity: Actions and interactions occurring within a computer network.

Network Traffic: The flow of data packets transmitted over a computer network.

NIST 800-53: A set of security and privacy controls published by the National Institute of Standards and Technology (NIST) for federal information systems and organizations.

Prevention: Activities and measures aimed at preventing cybersecurity incidents and mitigating potential risks.

Protection: Measures implemented to safeguard critical infrastructure and key resources from cybersecurity threats.

Public-Private Partnerships: Collaborative efforts between public and private sector organizations to address cybersecurity challenges and share resources.

Real-Time Indicator Feeds: Timely and up-to-date information feeds containing indicators of emerging cyber threats and vulnerabilities.

Recovery: Activities undertaken to restore and recover systems and operations following a cybersecurity incident.

Response: Coordinated efforts to address and mitigate the effects of cybersecurity incidents when they occur.

Risk Assessment: The process of identifying, analyzing, and evaluating potential risks and vulnerabilities to determine their potential impact and likelihood.

Security Patches and Updates: Software updates or fixes released by vendors to address identified vulnerabilities and enhance system security.

Self-Assessment: An evaluation conducted by grantees themselves to assess their own cybersecurity preparedness and identify areas for improvement.

SLTTs (State, Local, Tribal, and Territorial): Refers to the collective entities comprising state governments, local governments, tribal governments, and territorial governments.

Stakeholder Preparedness Review (SPR): A federally required review conducted every three years to assess the preparedness of stakeholders in addressing threats and hazards.

Territorial Government: The governing body responsible for the administration and governance of a specific territory or territorial possessions under the jurisdiction of a country.

Threat and Hazard Identification and Risk Assessment (THIRA): A federally required assessment conducted every three years to identify and evaluate threats, hazards, and risks.

Threat Mitigation Practices: Measures and actions taken to reduce or eliminate cybersecurity risks and threats.

Traffic Light Protocol (TLP): A framework used to classify and control the dissemination of sensitive incident-related information.

Tracking: The process of tracing and recording the movement or progress of something.

Tribal Government: The governing body responsible for the administration and governance of Native American tribes or indigenous communities within a country.

Vulnerability Management: The process of identifying, assessing, and addressing vulnerabilities in information systems, applications, and user accounts.

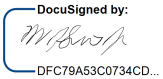
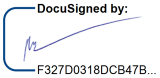
DocuSign

Certificate Of Completion

Envelope Id: E85C5188711042D281F52623E8DDFF10
Status: Completed
Subject: Complete with DocuSign: SoA SLCGP Cybersecurity Plan (Final Draft).docx
Source Envelope:
Document Pages: 34
Signatures: 2
Envelope Originator:
Certificate Pages: 4
Initials: 0
Bill Smith
AutoNav: Enabled
PO Box 110206
EnvelopeId Stamping: Disabled
Juneau, AK 99811
Time Zone: (UTC-09:00) Alaska
bill.smith@alaska.gov
IP Address: 158.145.14.25

Record Tracking

Status: Original
8/10/2023 2:48:48 PM
Holder: Bill Smith
bill.smith@alaska.gov
Location: DocuSign
Security Appliance Status: Connected
Pool: StateLocal
Storage Appliance Status: Connected
Pool: State of Alaska
Location: DocuSign

Signer Events	Signature	Timestamp
Bill Smith bill.smith@alaska.gov CIO State of Alaska Office of Information Technology Security Level: Email, Account Authentication (None)	DocuSigned by:  DFC79A53C0734CD... Signature Adoption: Uploaded Signature Image Using IP Address: 10.2.15.7	Sent: 8/10/2023 2:50:34 PM Viewed: 8/10/2023 2:50:44 PM Signed: 8/10/2023 2:50:55 PM
Electronic Record and Signature Disclosure: Accepted: 3/9/2022 11:45:27 AM ID: bc6ab434-c70f-461d-9daf-26bbb2fbe1a5 Company Name: State of Alaska		
Bryan J Fisher b.fisher@alaska.gov Security Level: Email, Account Authentication (None)	DocuSigned by:  F327D0318DCB47B... Signature Adoption: Uploaded Signature Image Using IP Address: 158.145.14.24	Sent: 8/10/2023 2:50:56 PM Viewed: 8/10/2023 3:19:23 PM Signed: 8/10/2023 3:19:53 PM
Electronic Record and Signature Disclosure: Accepted: 8/10/2023 3:19:23 PM ID: 1a8da33d-2794-4ad4-bac5-a356a3c0f9f6 Company Name: State of Alaska		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Bill Dennis bill.dennis@alaska.gov Administrative Operations Manager Security Level: Email, Account Authentication (None)	COPIED	Sent: 8/10/2023 3:19:55 PM

Carbon Copy Events	Status	Timestamp

Electronic Record and Signature Disclosure:
Accepted: 5/24/2021 7:33:16 AM
ID: 41c94d05-9122-462a-bc2a-1005b430e143
Company Name: State of Alaska

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/10/2023 2:50:34 PM
Certified Delivered	Security Checked	8/10/2023 3:19:23 PM
Signing Complete	Security Checked	8/10/2023 3:19:53 PM
Completed	Security Checked	8/10/2023 3:19:55 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

Please read this Electronic Records and Signature Disclosure (ERSD). It concerns your rights regarding electronically undertaking, and the conditions under which you and the State of Alaska agree to electronically undertake, the transaction to which it relates (the "TRANSACTION").

Consent to Electronically Undertake the TRANSACTION

You can electronically undertake the TRANSACTION only if you confirm that you meet the following requirements by selecting the box next to "I agree to use electronic records and signature" (the "AGREE BOX"):

1. you can fully access and have read this ERSD;
2. you can fully access all of the information in the other TRANSACTION records;
3. you can retain all of the TRANSACTION records in a form that you will be able to fully access for later reference;
4. you consent to undertake the TRANSACTION electronically; and
5. you are authorized to undertake the TRANSACTION. (Please note that falsely undertaking the TRANSACTION may subject you to civil liabilities and penalties and/or to criminal penalties.)

If you cannot or are not willing to confirm each of these five things, do not select the AGREE BOX.

Withdrawing Consent

If you select the AGREE BOX, you can withdraw your consent to electronically undertake the TRANSACTION at any time before you complete the TRANSACTION: simply do not finalize it. The only consequence of withdrawing your consent is that you will not finalize the TRANSACTION.

If you select the AGREE BOX, your consent will apply only to this TRANSACTION. You must separately consent to electronically undertake any other transaction with the State of Alaska.

Paper Option for Undertaking the TRANSACTION

You may undertake the TRANSACTION with the State of Alaska using paper records. (State of Alaska employees who want to undertake the TRANSACTION in paper should contact the agency responsible for the TRANSACTION.) Print the paper records on the website of the State of Alaska agency responsible for the TRANSACTION, or request them from the agency. The State of Alaska homepage is at http://alaska.gov/.

Copies of TRANSACTION Records

After completing the TRANSACTION but before closing your web browser, you should download the TRANSACTION records. Or you can download the records within 30 days after

completing the TRANSACTION using the link in the DocuSign email sent to the email address you used to complete the TRANSACTION. The State of Alaska will not provide a paper copy of the TRANSACTION records as part of the TRANSACTION. Under the Alaska Public Records Act (APRA), AS 40.25.100–.295, you can request a copy from the agency responsible for the TRANSACTION, but if too much time has passed, the agency may no longer have the records when you make your request. If required under the APRA, the agency will charge a fee.

Required Hardware and Software

For the minimum system requirements to electronically undertake the TRANSACTION, including accessing and thereby retaining the TRANSACTION records, visit https://support.docusign.com/guides/signer-guide-signing-system-requirements. These requirements may change. In addition, you need access to an email account.

How to Contact the State of Alaska

To ask a question on this ERSD or the DocuSign document generated after you complete the TRANSACTION or on using DocuSign to electronically undertake the TRANSACTION, contact the Alaska Department of Administration at either of the following addresses:

State of Alaska
Department of Administration
550 West 7th Avenue
Suite 1970
Anchorage, AK 99501
Reference: DocuSign

doa.commissioner@alaska.gov
Subject: DocuSign

To ask any other question on the TRANSACTION records or to update the information for contacting you electronically, contact the State of Alaska agency responsible for the TRANSACTION using the contact information in the TRANSACTION records or, if those records contain no contact information, using the contact information on the agency's website. Again, the State of Alaska homepage is at http://alaska.gov/.

File #: 24-0097, **Version:** 1

ITEM TITLE:
Information Technology Department Annual Report

SUBMITTED BY: Matthew Osburn, IT Director

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Receive and file.

SUMMARY STATEMENT:

The IT Department will present their annual department report to the council. The presentation is included as an attachment.

City of VALDEZ

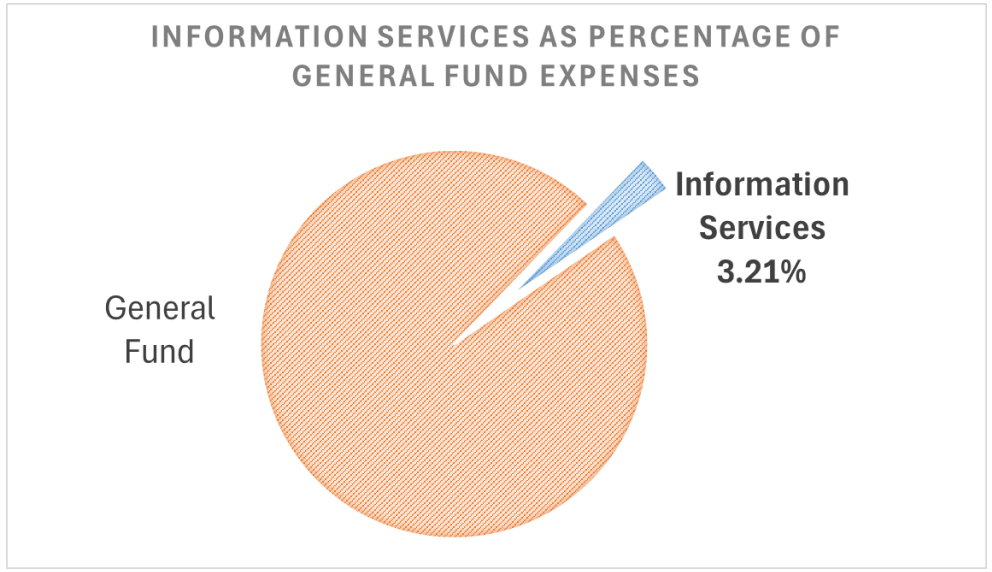
Department Report

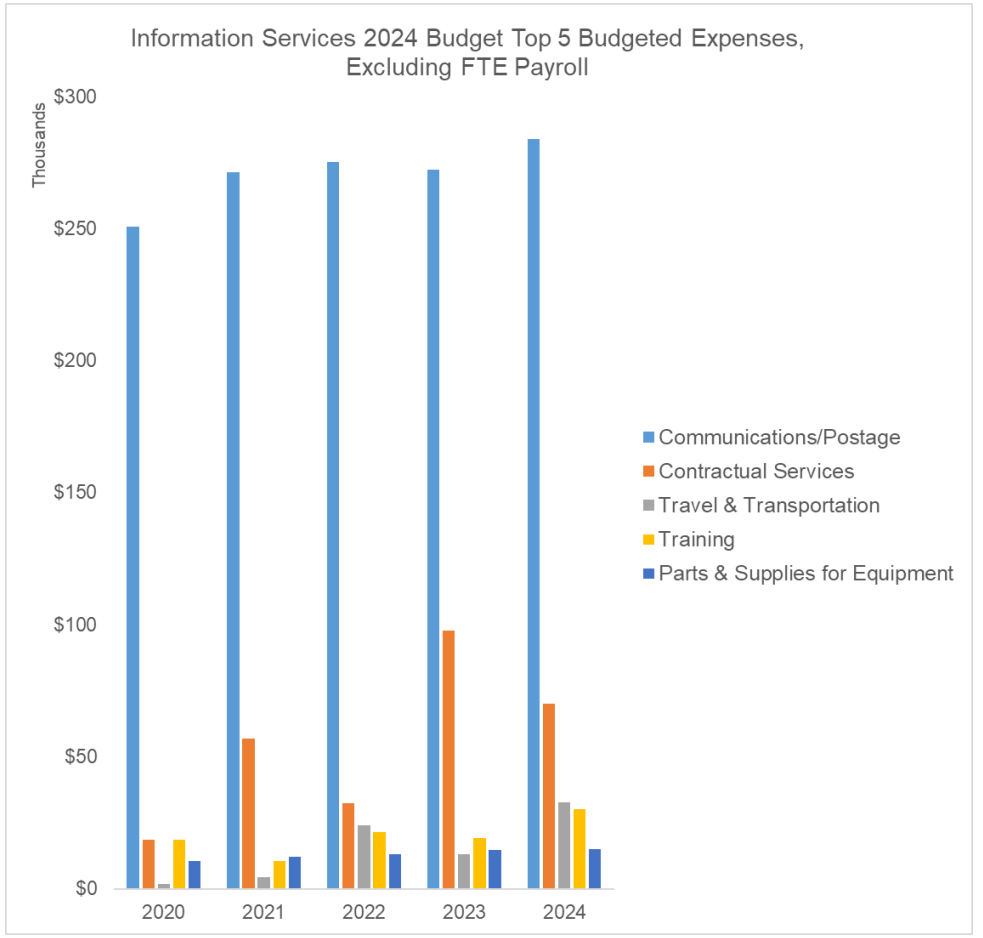
Information Services 2024

2024 Big Picture

Communications Services includes Dark Fiber Lease

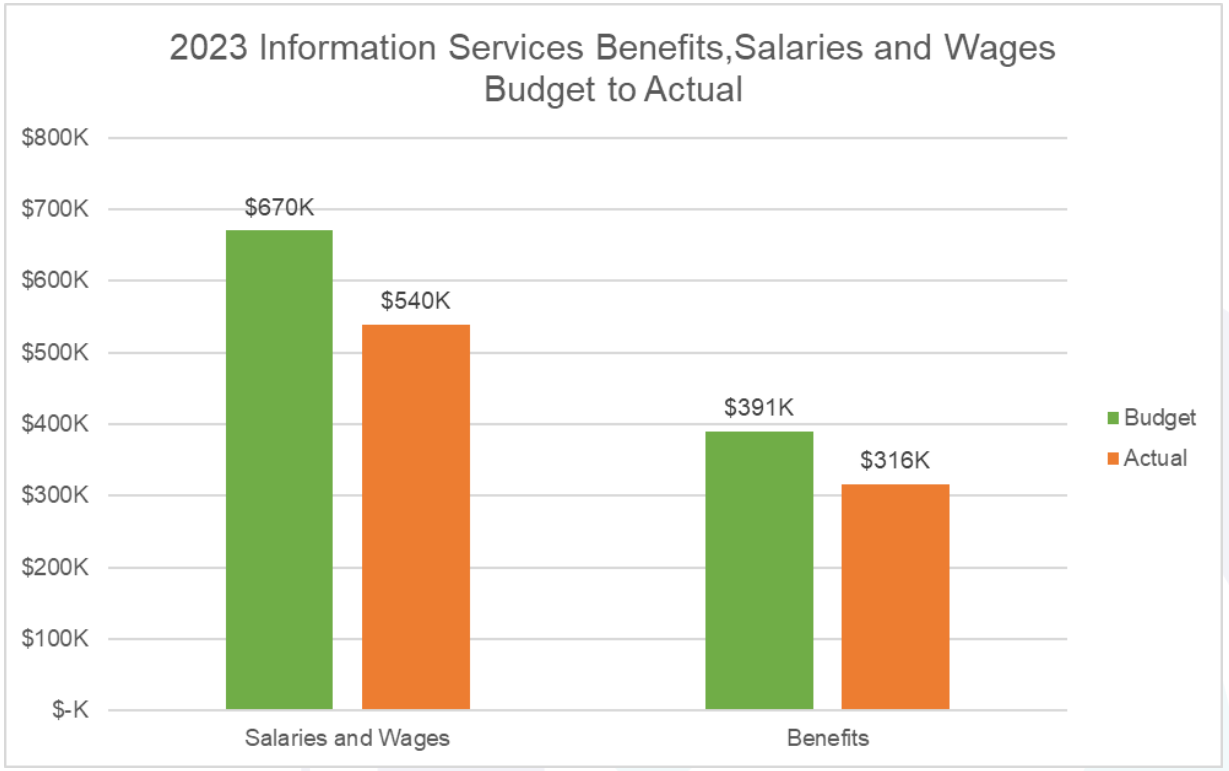
Communications and Contractual are mix of City wide and departmental costs





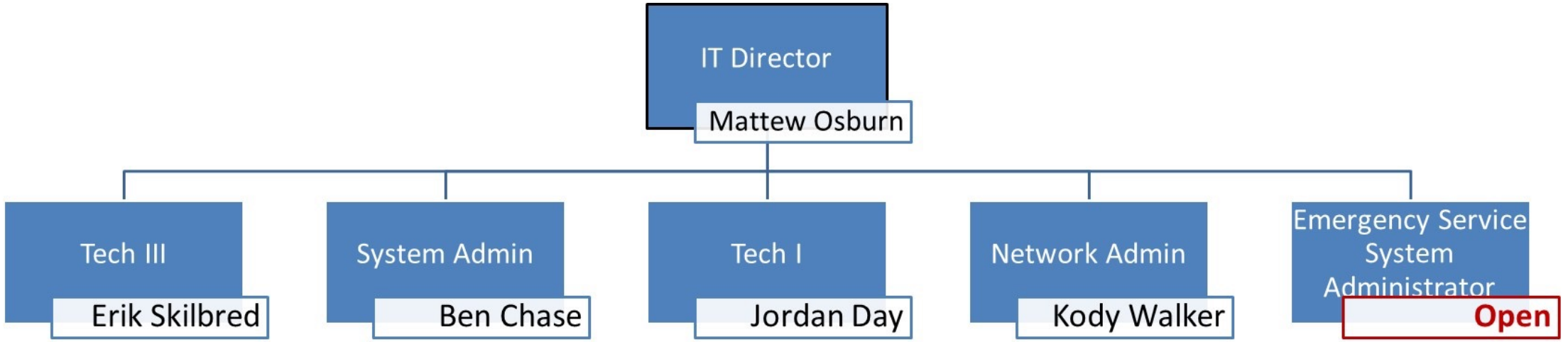
Personnel History; Information Services Department

One Open FTE Position
Department Exempt Positions



Authorized Position Count	2020	2021	2022	2023	2024
Administration	**30**	**30**	**30**	**30**	**30**
ADMINISTRATION	2.8	2.8	2.8	2.8	2.8
CITY CLERK	5	5	5	5	5
CITY COUNCIL	0	0	0	0	0
ECONOMIC DEVELOPMENT	2.2	2.2	2.2	1.2	1.2
FINANCE	6	6	6	6	6
HUMAN RESOURCES	2	2	2	2	2
INFORMATION SERVICES	5	5	5	6	6
PLANNING	7	7	7	7	7

Personnel; Information Services Department



IT Director: Ensures the department's streamlined operation aligns with the city, state, and federal objectives. Oversight of technical procurement.

Systems Administrator: Responsible for Servers, Cloud Services, and VMs. Cyber Security

Emergency Service SA: IT department operations but with a focus on PD, Fire, and EM support.

Network Administrator: Maintains and monitors firewalls, switches, and other network systems. Has core responsibilities with cyber security operations.

IT Tech I, II, III: This frontline worker focuses on the helpdesk, customer care, and systems deployment. Depending on the level, he or she is responsible for different project levels.

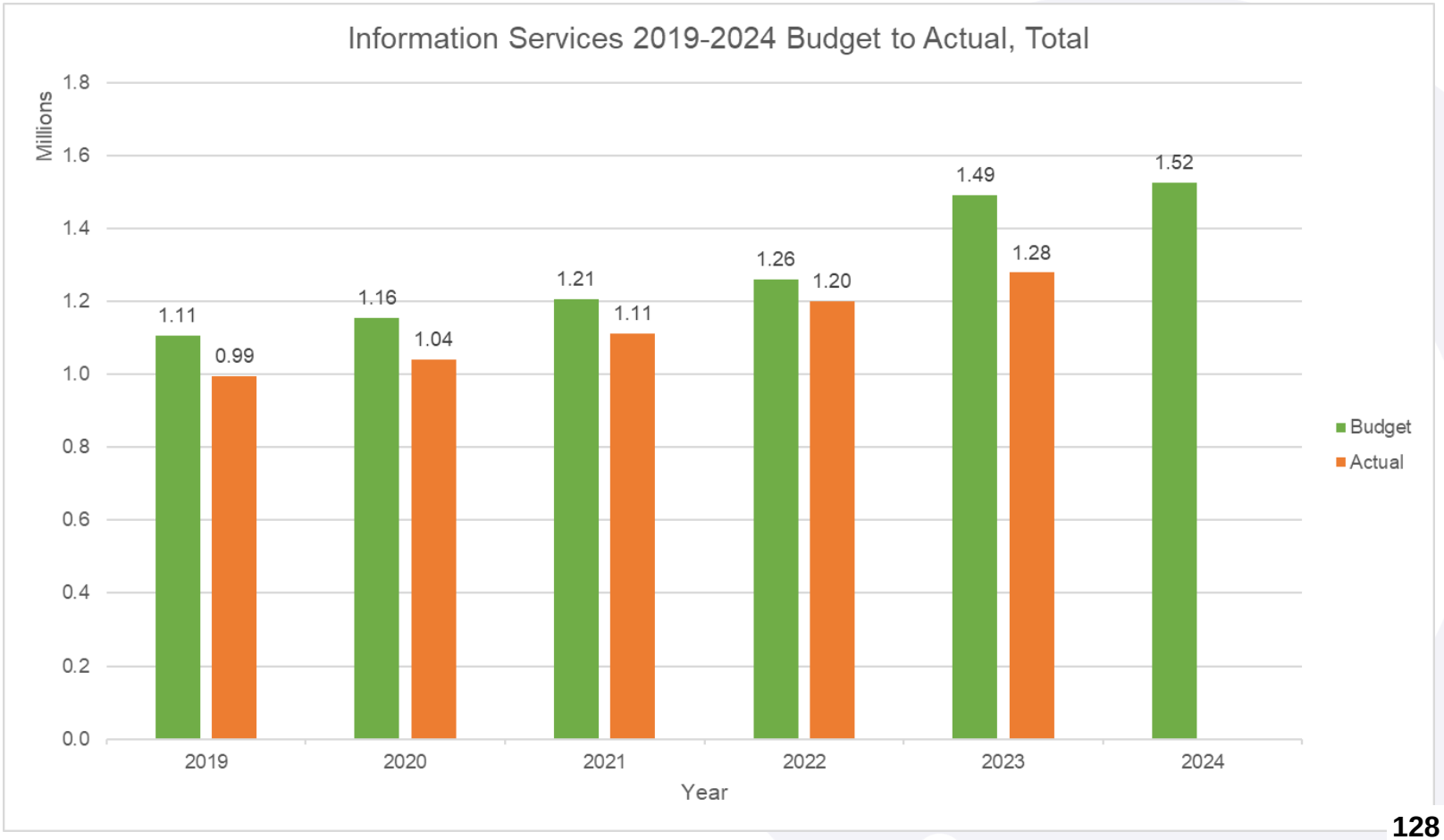
Budget to Actual 2019-2024

Tech Reserve – Like Major Equipment

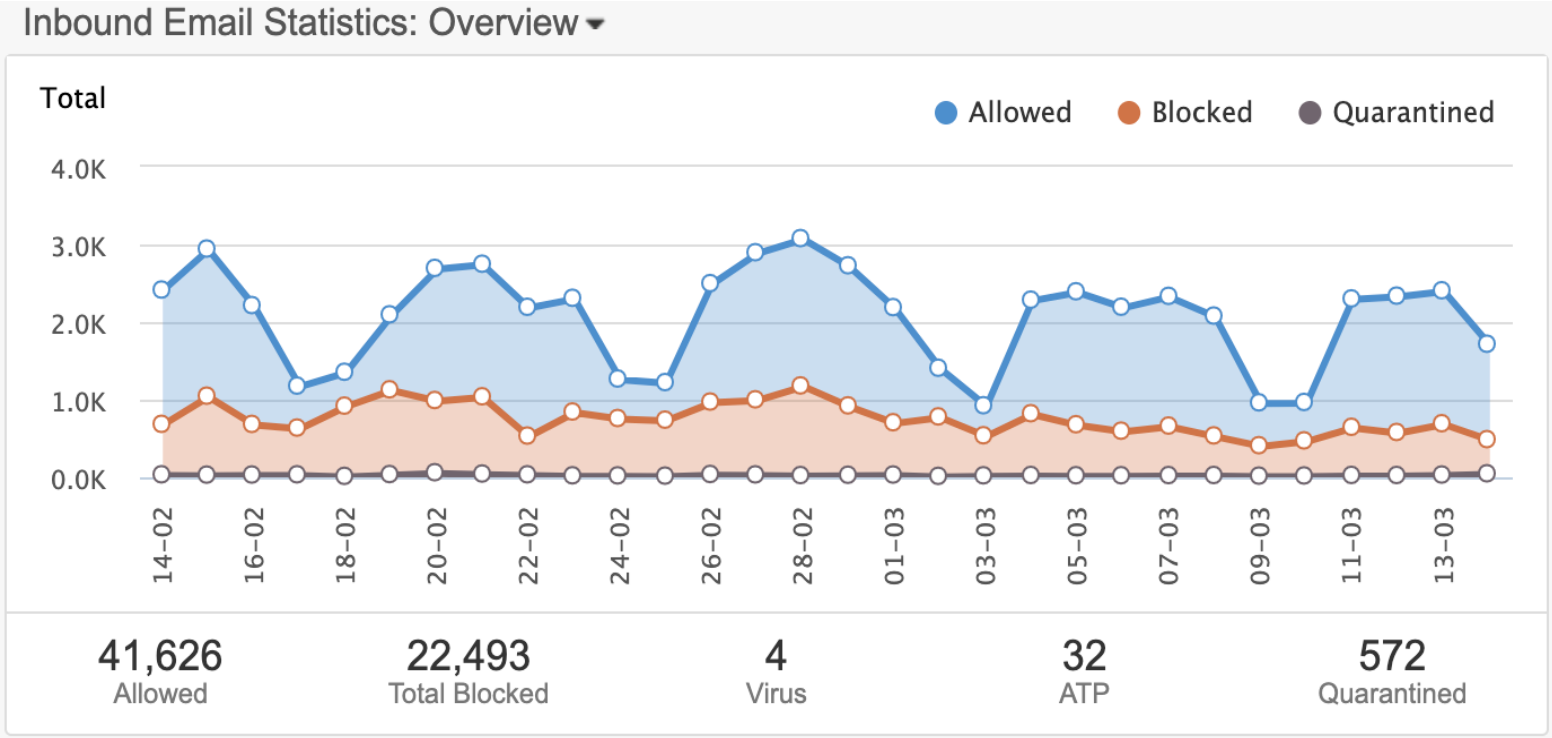
Renewals and goods are increasing by 5% to 10% on average.

Fewer services provided by the State

Funded on a 5-year average



Information Services KPI

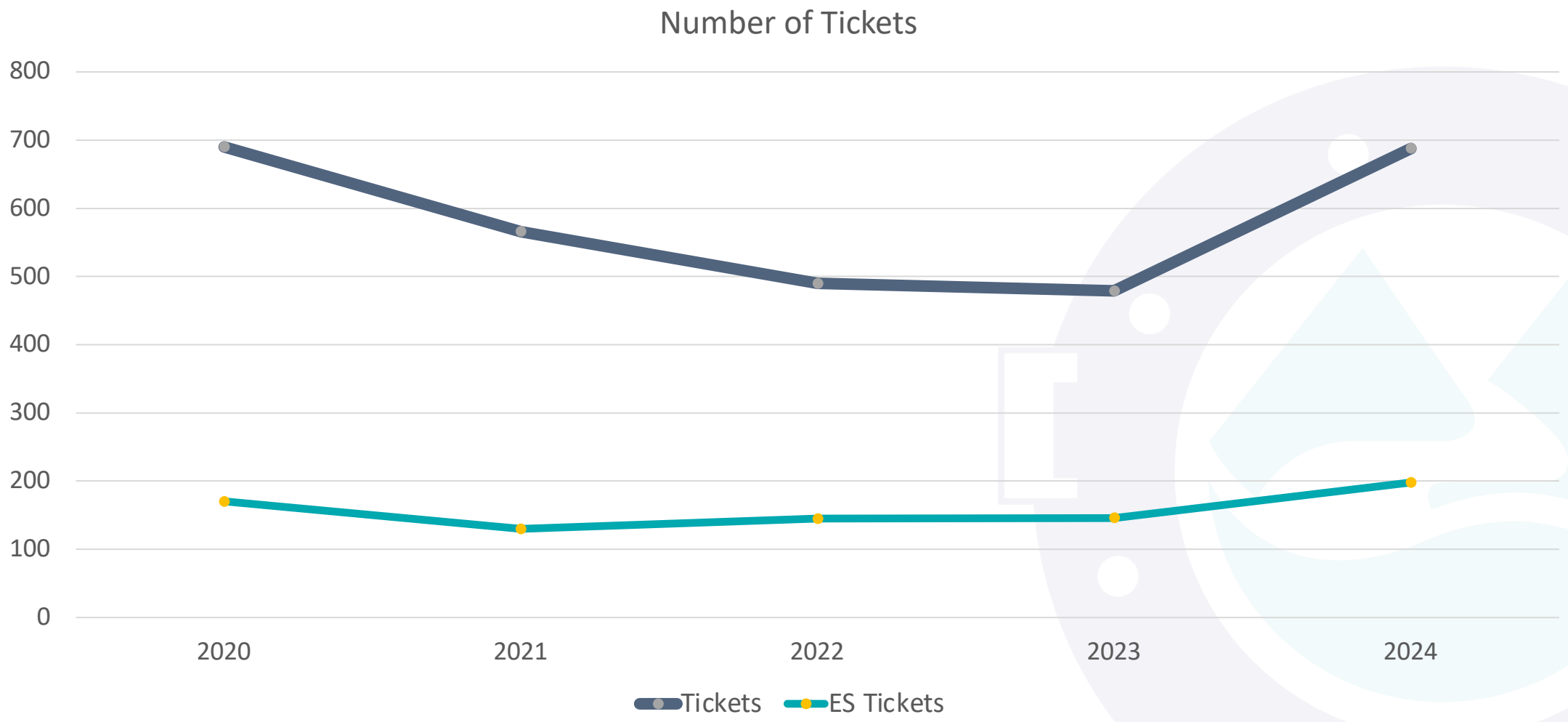


5 FTE – **1 Unfilled Position**

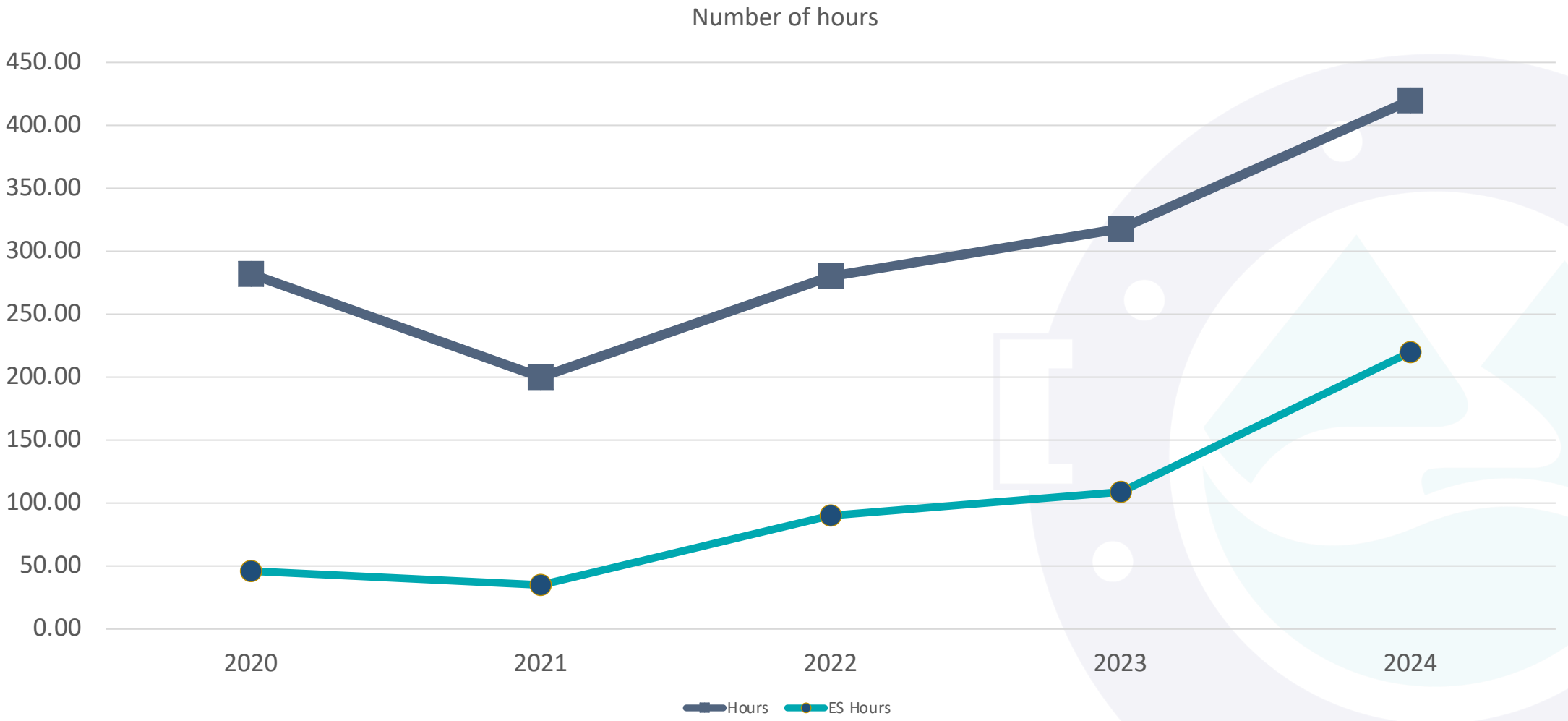
Infrastructure

- **200 Computers/ End devices**
- **138 Mobile Devices**
- **55 Network Devices**
- **45 Virtual Machines**
- **14 Buildings/Locations**
- **10 Servers (reduced from 21)**

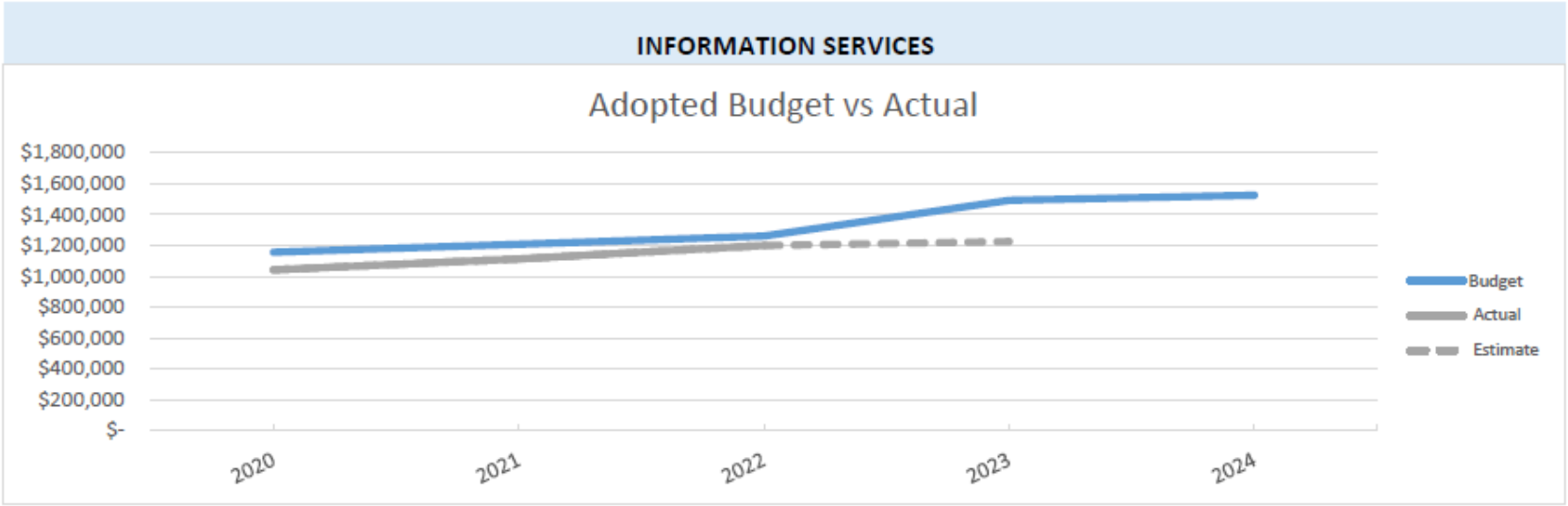
IT Tickets from 2019-2024



IT Hours 2019-2024



2025 Budget; Information Services Department

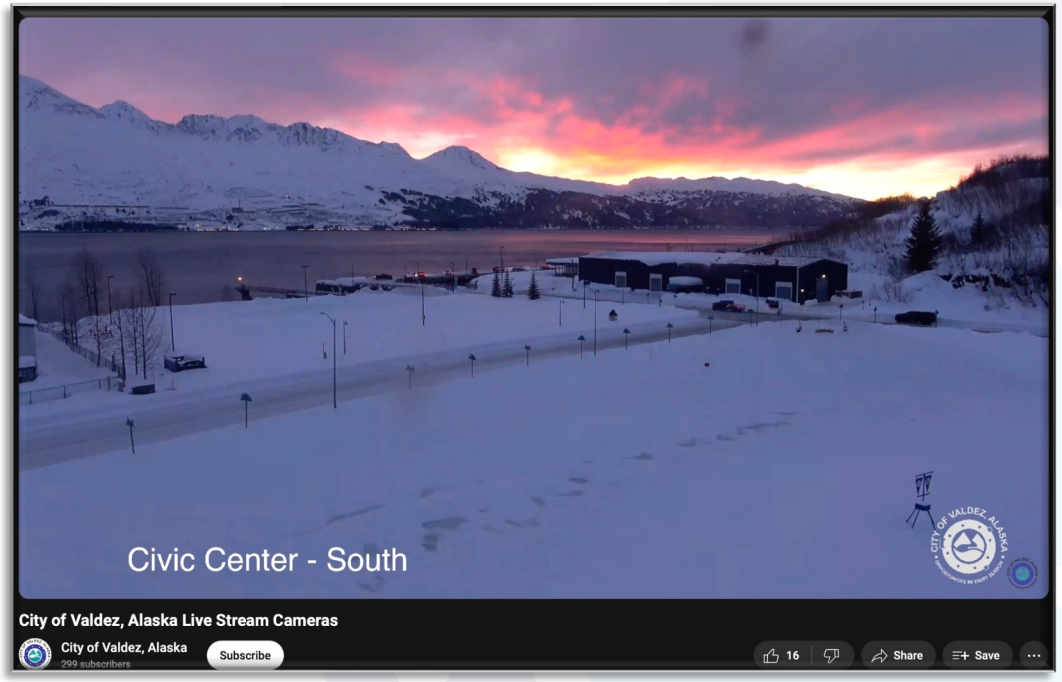


Over 3%
0-3%
Below 0%

Expenses	Actual Expenditure			Estimate	Adopted Budget		2023 to 2024 Budget Changes	
	2020	2021	2022	2023	2023	2024	Dollar Change	Percent Change
FTE Payroll	721,010	744,565	819,748	832,675	1,060,623	1,076,156	15,533	1.5%
Other Personnel	22,035	15,890	46,664	38,450	63,860	63,800	(60)	-0.1%
Other Operating	279,643	293,904	300,084	298,200	303,300	314,300	11,000	3.6%
Contracts	18,651	56,800	32,413	55,000	64,000	70,000	6,000	9.4%
Grand Total	1,041,339	1,111,159	1,198,909	1,224,325	1,491,783	1,524,256	32,473	2.2%

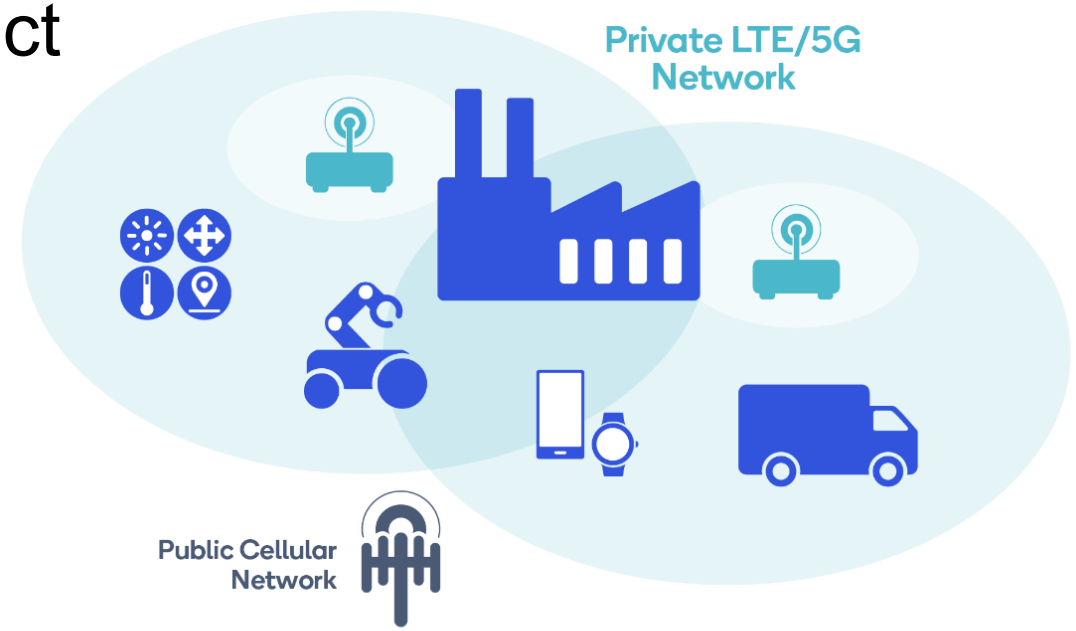
IT 2024 Tasks

- Redundant Satellite Internet
- Complete Wi-Fi deployment
- Public YouTube Feed
- Staffing
- Cyber Security Grant



IT 2025 Tasks

- Staffing Challenges
- Core Communications
  - Private LTE
  - Radio Infrastructure Project
- Cyber Security Assessment



File #: 24-0099, **Version:** 1

ITEM TITLE:
Monthly Treasury Report: January, 2024
SUBMITTED BY: Casey Dschaak, Budget and Financial Analyst

FISCAL NOTES:

Expenditure Required: n/a
Unencumbered Balance: n/a
Funding Source: n/a

RECOMMENDATION:

Receive and file

SUMMARY STATEMENT:

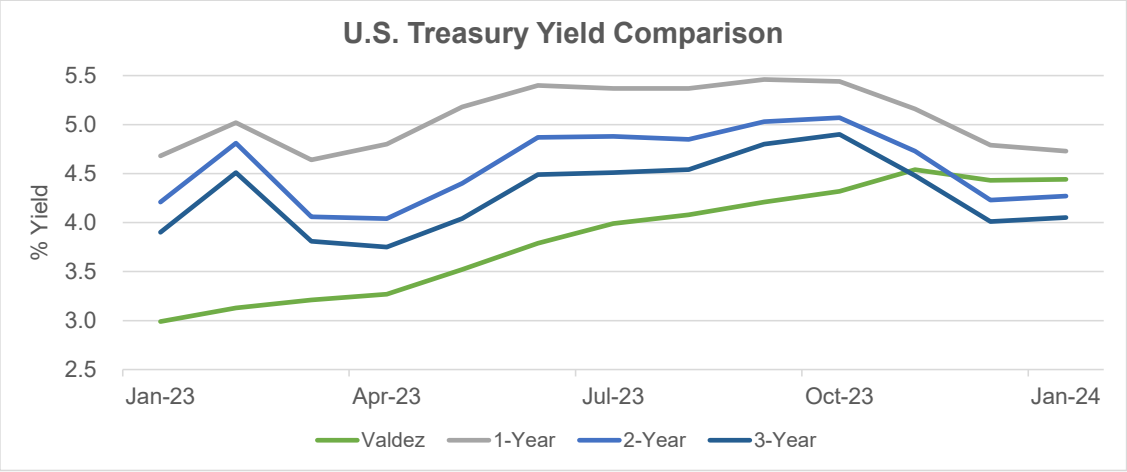
Monthly treasury report per municipal code

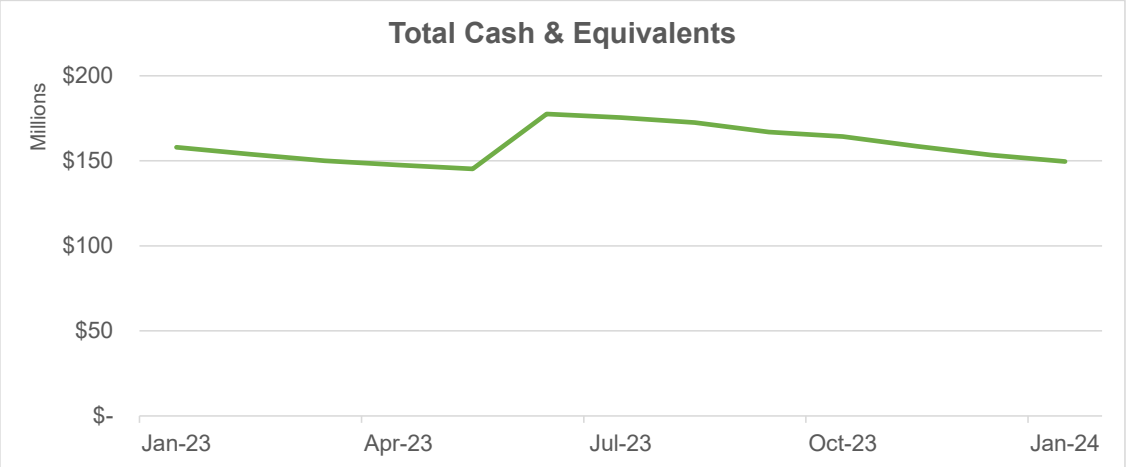
Monthly Treasury Report

Period Ending: **January 31, 2024**

Prepared By: *Casey Dschaak, Financial Analyst*

		Begin Balance	Debits	Credits	End Balance	Yield	Notes
Central Treasury		**153,414,201**	**16,610,203**	**(20,497,875)**	**149,526,528**	**4.44%**	
Central Treasury	Principal	95,336,237	323,969	-	95,660,206	3.92%	
Money Market	Wells Fargo	58,379,129	295,658	(4,750,000)	53,924,787	5.27%	
Checking	Wells Fargo	(195,087)	14,061,778	(13,898,079)	(31,387)	0.00%	
Payroll	Wells Fargo	(106,079)	1,928,797	(1,849,796)	(27,078)	0.00%	
Sweep	Wells Fargo	789,364	7,260,760	(4,253,661)	3,796,463	5.18%	
Restricted		**4,749**	**4**	**-**	**4,753**	**0.00%**	
Debt Service	Principal	-	-	-	-	0.00%	
Police	Wells Fargo	4,749	4	-	4,753	0.00%	
Total		**153,418,949**	**16,610,207**	**(20,497,875)**	**149,531,281**	**4.44%**	





File #: 24-0100, **Version:** 1

ITEM TITLE:
Legal Billing Summary - February 2024

SUBMITTED BY: Elise Sorum-Birk, Deputy City Clerk

FISCAL NOTES:

Expenditure Required: N/A
Unencumbered Balance: N/A
Funding Source: N/A

RECOMMENDATION:

Receive and file.

SUMMARY STATEMENT:

Attorney billing summary for February 2024 is attached for City Council review.

BRENA, BELL & WALKER, P.C.

ROBIN O. BRENA, MANAGING ATTORNEY
JESSE C. BELL
WILLIAM M. WALKER
DAVID W. WENSEL
ANTHONY S. GUERRIERO
JON S. WAKELAND
KELLY M. MOGHADAM
JAKE W. STASER

ATTORNEYS AT LAW

810 N STREET, SUITE 100
ANCHORAGE, ALASKA 99501
TELEPHONE: (907) 258-2000
FACSIMILE: (907) 258-2001
WEB SITE: BRENALAW.COM

trupe@brenalaw.com

March 14, 2024

City of Valdez
Attn: John Douglas, City Manager
P.O. Box 307
Valdez, AK 99686

February 2024 Billing Summary Sheet

File No.	Description	Amount
1374-007	City Council	$2,372.50
1374-008	Capital Facilities	$325.00
1374-009	Ports & Harbors	$65.00
1374-011	Administration	$3,932.50
1374-012	Community Development	$3,482.97
1374-014C	Escaped Property 2017-2022 Superior Court Appeal Case No. 3AN-22-06115CI Fees $255,214.75 Experts $180,698.67 Additional Costs $ 21,673.86	$457,587.28
1374-016	Parks and Recreation	$65.00
1374-017	Police Department	$455.00
1374-018	Human Resources CONFIDENTIAL	$3,890.46
1374-042	Redistricting	$1,460.20
1374-044	Alaska Trappers	$97.50
1374-049	Alderwood Litigation, 3VA-22-00059 CI	$391.00
	TOTAL	$474,124.41

Contributed-Hour Summary

DO NOT PAY - Fees will be paid from any attorneys' fees award.

File No.	Description	Fees Over Cap
1374-043A	City of Valdez/RCA/Appeal of Order 6 Superior Ct. No. 3AN-20-05915 CI Work began March 2020 Initial Fee Cap of $45,000 has been met.	$72,358.66
1374-043B	City of Valdez/RCA/Consolidated Appeals of Orders 6 & 17 Superior Ct. Nos. 3AN-20-05915 CI/3AN-21-04104 CI (Consolidated) Work began December 2020 Initial Fee Cap of $25,000 has been met.	$276,274.50
1374-043C	City of Valdez/BP-Hilcorp/Dismissal Appeal Supreme Ct. No. S-18178 Work began August 2021	$302,667.52
1374-043D	City of Valdez/BP-Hilcorp/Constitutional Claimant Fees Appeal, Supreme Ct. No. S-18347 Work began February 2022	$109,014.09
	TOTAL	$760,314.77

STATE OF ALASKA

STATEWIDE

CYBERSECURITY STRATEGIC

PLAN (SCSP)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM CYBERSECURITY PLANNING COMMITTEE 2

CYBERSECURITY PLAN ELEMENTS 6

ENHANCE PREPAREDNESS 9

FUNDING & SERVICES 16

ASSESS CAPABILITIES 16

IMPLEMENTATION PLAN 17

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT 19

APPENDIX B: PROJECT SUMMARY WORKSHEET 23

APPENDIX C: ENTITY METRICS 24

APPENDIX D: ACRONYMS 26

APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES 27

APPENDIX F: KEY TERMS AND DEFINITIONS 29

LETTER FROM CYBERSECURITY PLANNING COMMITTEE

Dear Cybersecurity Practitioners,

On behalf of the Alaska State and Local Cybersecurity Grant Program (SLCGP) Planning Committee I am pleased to introduce the 2023 Statewide Alaska Cybersecurity Strategic Plan. This plan reflects the State's continued dedication to enhancing cybersecurity and supporting the public entities within Alaska, as well as collaborating with our local partners.

The Cybersecurity Plan was developed through a collaborative effort of the State of Alaska (SOA) boroughs, cities, tribes, public education, and health institutions throughout the state. It incorporates best practices for managing cybersecurity risks and includes actionable and measurable goals and objectives focusing on the following priorities:

1. Enhance Cybersecurity Resilience and Interoperability
2. Foster a Cybersecurity Culture
3. Strengthen Cybersecurity Collaboration and Partnerships
4. Improve Cyber Incident Management and Response Capabilities

These goals and objectives are designed to help us navigate the ever-changing cybersecurity landscape and plan for new technologies. The Cybersecurity Plan aligns with the requirements of the U.S. Department of Homeland Security for the State and Local Cybersecurity Grant Program (SLCGP) and will serve as a reference point to help evaluate grants requested under that program. In addition, it is a powerful resource to provide practical guidance, coordination, and common understanding throughout the public sector in Alaska.

We recognize the importance of collaboration across disciplines and jurisdictions. Our plan emphasizes the need for partnership and information sharing with local governments, tribes, federal agencies, private sector, academic institutions, and non-profit organizations.

We are committed to achieving the goals outlined in the Cybersecurity Plan and to increase Alaska's cyber resilience. With the help of cybersecurity practitioners and engaged leaders, we can continue to improve our resilience and ensure the safety and security of our state's critical systems and information.

Thank you for your efforts to improve cybersecurity performance throughout the state. We look forward to continuing to work with you to achieve our cybersecurity objectives.

Sincerely,

DocuSigned by:

1DFC79A539D734CD...

Bill Smith
Chief Information Officer
State of Alaska | Department of Administration
Planning Committee Co-Chair

DocuSigned by:

F327D0318D0B47B...

Bryan J Fisher
State Authorized Agent
Planning Committee Co-Chair

INTRODUCTION

The State of Alaska Statewide Cybersecurity Strategic Plan (SCSP) is a key component to helping Alaska increase its cyber resilience. Representatives from across the spectrum of Alaska public sector agencies used existing plans, structures, and other relevant efforts to develop this comprehensive cybersecurity plan. Building upon existing structures and capabilities allows Alaska to provide governance and a framework to meet Alaska's critical cybersecurity needs while making the best use of available resources. Members of the planning committee consulted with local governments and associations of local governments and incorporated their feedback into this cybersecurity plan through a collaborative approach. The Department of Military and Veteran Affairs and the Office of the CIO in the Department of Administration partnered to form a Statewide Alaska Cybersecurity Strategic Plan Support Team. The support team established regular communication channels with local governments to gather feedback and input on the cybersecurity plan. This involved holding regular meetings to discuss cybersecurity challenges, share best practices, and gather feedback. This plan represents a baseline that will continue to improve and evolve over time, incorporating continuous input and responding to the ever-changing threat landscape. It is designed to focus on common principles that will help build a strong foundation across all levels of public agencies.

The SCSP support team recognizes the importance of involving these stakeholders in the cybersecurity planning process and ensured that their perspectives and insights were incorporated into the plan. By incorporating feedback from local jurisdictions, the State of Alaska meets requirements **SLCGP: e.2.A.ii.**

The Cybersecurity Plan is a two-year strategic planning document that contains the following components:

- **Vision and Mission**: The vision of the plan is to enhance Alaska's cybersecurity posture and resilience to mitigate cyber threats and vulnerabilities. The mission is to develop and implement a comprehensive cybersecurity strategy that involves all stakeholders and ensures the safety and security of Alaska's critical infrastructure and systems.
- **Organization, and Roles and Responsibilities:** This section describes the current roles and responsibilities for cybersecurity within the state, including any governance mechanisms in place. It also identifies the successes, challenges, and priorities for improvement. The plan outlines a strategy for the cybersecurity program and the organization structure that supports it. Additionally, the governance framework outlines authorities and requirements for the cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any state or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** The plan describes how feedback and input from local governments and associations were incorporated to reduce overall cybersecurity risk across Alaska. This was achieved through stakeholder engagement, meetings, and workshops, to ensure a holistic approach to developing the cybersecurity plan.
- **Cybersecurity Plan Elements:** This section outlines the technology and operations needed to maintain and enhance resilience across the cybersecurity landscape. The plan includes the 16 required elements outlined in the State and Local Cybersecurity

Improvement Act, including managing, monitoring, and tracking information systems, enhancing preparation and response to incidents, implementing continuous cybersecurity risk management practices, adopting best practices and methodologies, promoting the delivery of safe and trustworthy online services, ensuring continuity of operations, enhancing the cybersecurity workforce, and mitigating risks to critical infrastructure and key resources.

- **Funding:** The plan describes funding sources and allocations to build cybersecurity capabilities within the state, along with methods and strategies for funding sustainment and enhancement to meet long-term goals. This includes using cybersecurity grant funding to provide cost-effective and scalable cybersecurity services to local governments, including rural communities.
- **Implementation Plan:** The plan describes the state's approach to implementing, maintaining, and updating the Cybersecurity Plan to enable continued evolution and progress toward the identified goals. It includes a timeline for implementation and identifies the necessary resources needed to achieve the plan's objectives.
- **Metrics:** The plan describes how the state will measure the outputs and outcomes of the program across the state, including the use of key performance indicators (KPIs) to measure progress against the identified goals. This includes tracking the number of assessments, audits, exercises, and training sessions conducted, as well as the number of entities completing each component of the curriculum.

Vision and Mission

Alaska's vision and mission for improving cybersecurity practices statewide:

Vision:

Create a secure and resilient cybersecurity environment for the State of Alaska, where all state, local, and tribal governments work together seamlessly to protect against cybersecurity risks and threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

Mission:

Develop and implement a comprehensive cybersecurity plan for the State of Alaska that incorporates existing plans and feedback from local governments, promotes the adoption of best practices and methodologies, and ensures the continuity of operations in the event of a cybersecurity incident. The outcomes form this planning effort and implementation will include: assessment of the capabilities of the eligible entity relating to the actions described in the plan and identify and mitigate any gaps in the cybersecurity workforce, enhancement of the delivery of safe and trustworthy online services and work to establish strong partnerships to improve information sharing and collaboration. , and collaboratively striving to achieve measurable progress towards reducing cybersecurity risks and identifying, responding to, and recovering from

cybersecurity threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

Cybersecurity Program Goals and Objectives

State of Alaska Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. **Enhance Cybersecurity Resilience and Interoperability.** Encourage and support cybersecurity resilience by promoting the adoption of risk management programs that incorporate best practices and methodologies. Encourage alignment of information and operational technology cybersecurity objectives, and advocate for the establishment of an information and operational technology modernization cybersecurity review process.	1.1 Support and encourage a cybersecurity risk assessment of state and local government information systems to identify vulnerabilities and develop a risk management plan. Support the establishment of risk assessment protocols and provide guidance and resources to aid in the identification of potential cybersecurity risks and vulnerabilities. 1.2 Support and encourage the implementation of a continuous monitoring program to identify and mitigate cybersecurity risks and threats to information systems owned or operated by the state or local governments within Alaska. Promote the adoption of continuous monitoring practices and provide support to organizations and agencies in their efforts to identify and mitigate potential cybersecurity risks and threats.
2. **Foster a Cybersecurity Culture.** Encourage and support the fostering of a cybersecurity culture by promoting awareness and training programs for state employees, contractors, and local government personnel. Encourage the adoption of such programs and support the efforts of organizations and agencies in providing cybersecurity education and training to their employees and stakeholders.	2.1 Support and encourage the development and delivery of cybersecurity awareness and training programs to state employees, contractors, and local government personnel. Promote the adoption of such programs and provide resources and guidance to aid in the development and delivery of effective cybersecurity education and training. 2.2 Support and encourage the establishment of a cybersecurity awareness program to educate citizens on best practices and cybersecurity risks. Advocate for the adoption of awareness programs and provide resources and guidance to organizations and agencies in their efforts to educate citizens on cybersecurity risks and promote best practices.

Program Goal	Program Objectives
3. **Enhance Cybersecurity Collaboration and Partnerships.** Support and encourage the enhancement of Cybersecurity Collaboration and Partnerships by promoting the development of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and fostering cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations. Advocate for the establishment of information sharing protocols and encourage organizations and agencies to form partnerships and collaborations that promote effective cybersecurity practices and information sharing.	3.1 Support and encourage the development and implementation of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies. Advocate for the establishment of information sharing protocols and provide resources and guidance to organizations and agencies in their efforts to develop and implement effective information sharing programs. 3.2 Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations to develop and implement best practices.
4. **Improve Cybersecurity Incident Management and Response Capabilities.** Support and encourage the development and implementation of a cybersecurity incident response plan that outlines the roles, responsibilities, and procedures for responding to and recovering from cybersecurity incidents. Provide guidance and resources to aid in the establishment of incident response protocols and support organizations and agencies in their efforts to effectively respond to cybersecurity incidents.	3.3 Support and encourage the establishment of a cybersecurity incident response team with appropriate roles and responsibilities and promote the training and equipping of the team to respond to cybersecurity incidents. Provide resources and guidance to organizations and agencies in their efforts to establish incident response teams and ensure their readiness to respond to cybersecurity incidents. 3.4 Support and encourage the development and implementation of a cybersecurity incident management plan that outlines the procedures for responding to cybersecurity incidents and the roles and responsibilities of all stakeholders involved. Advocate for the adoption of incident management plans and provide support to organizations and agencies in their efforts to effectively respond to cybersecurity incidents.

CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

- State of Alaska Emergency Operations Plan (EOP) available at https://ready.alaska.gov/plans/
- State of Alaska 2023 -2025 Integrated Preparedness Plan (IPPW) available at https://ready.alaska.gov/Documents/Preparedness/Exercise/IPP%20SFY2023-2025.pdf
- Small Community Emergency Response Plan (SCERP), plan can be accessed by contacting the Alaska Division of Homeland Security and Emergency Management at mvaplanning@alaska.gov
- State of Alaska Hazard Mitigation Plan, available at https://ready.alaska.gov/Mitigation/SHMP

MANAGE, MONITOR, AND TRACK

The State of Alaska recognizes the critical importance of managing, monitoring, and tracking information systems, applications, and user accounts to effectively protect against cybersecurity risks and threats. To achieve this goal, the State will take – and encourage local governments to take – a comprehensive, integrated, and risk-based approach that incorporates the best practices and methodologies outlined in the Cybersecurity plan. Our strategic approach will focus on the following key areas.

Inventory Management

The State of Alaska encourages and supports the development of an inventory management program that includes all hardware and software used by the State, to include local government entities as feasible and decided locally. The inventory management program should incorporate prioritized risk to each item and should be reviewed and updated at least annually. This program will ensure that we have an accurate and up-to-date inventory of all information systems, applications, and user accounts, as well as any legacy systems that are no longer supported by the manufacturer. We encourage and support the development of policies and procedures for managing, monitoring, and tracking these systems to ensure that they are effectively protected against cybersecurity risks and threats.

Continuous Monitoring

The State of Alaska encourages and supports a continuous monitoring program that includes monitoring of activity, and behavior across all information systems, applications, and user accounts owned or operated by the State and encouraged for all local governments to implement and share. The program should leverage advanced technologies and tools to identify and mitigate cybersecurity risks and threats, including those that may target legacy systems. We also encourage and support the establishment of processes for responding to any alerts or incidents identified through the continuous monitoring program. The monitoring program should include identification of privileged accounts, key data and where it is stored and ensure it confidentiality, integrity, and availability.

Risk-Based Vulnerability Management

We encourage a risk-based vulnerability management program that includes regular vulnerability assessments and threat mitigation practices prioritized by the degree of risk to address cybersecurity risks and threats on all information systems, applications, and user accounts owned or operated by the state or local governments. This program should incorporate best practices and methodologies, to ensure that we are effectively managing, monitoring, and tracking vulnerabilities and threats.

Legacy System Management

We recognize that legacy systems that are no longer supported by the manufacturer are particularly vulnerable to cybersecurity threats. To address this vulnerability, we will encourage and support the implementation of a comprehensive legacy system management program that includes special focus on managing, monitoring, and tracking these systems to effectively protect, detect, respond to, and recover from cybersecurity incidents. This program should also include strategies for modernizing or replacing legacy systems where necessary.

While we understand that some eligible grant recipients may face constraints preventing them from replacing their legacy systems, we strongly encourage them to prioritize the implementation of compensating controls. Compensating controls serve as alternative measures to achieve cybersecurity objectives when traditional controls are not feasible or practical. By implementing these controls, entities

can mitigate the risks associated with legacy systems and reduce the likelihood and impact of cybersecurity incidents. We are committed to collaborating with such entities, assisting them in identifying and implementing compensating controls that are suitable for their specific needs and circumstances.

By adopting a comprehensive, integrated, and risk-based approach to managing, monitoring, and tracking information systems, applications, and user accounts, the State of Alaska will improve its cybersecurity resilience and interoperability over the next two years, and beyond. This approach will ensure that we are effectively protecting against cybersecurity risks and threats, including those that target legacy systems, and that we are able to detect, respond to, and recover from incidents in a timely and effective manner meet the requirement SLCGP: e.2.B.iv.

MONITOR, AUDIT, AND TRACK

The State of Alaska recognizes the importance of monitoring, auditing, and tracking network traffic and activity to enhance cybersecurity resilience across state and local government entities. While Alaska does not have a centralized security / information technology operation center (SOC / ITOC) to monitor, audit, and track network traffic and activity across all SLTTs currently, the state does support and encourage the following to monitor, audit, and track network traffic and activity:

- **Decentralized Monitoring:** SLTTS can be responsible for monitoring, auditing, and tracking their own network traffic and activity. This can be done using a combination of commercial and open-source tools and can be supplemented by training and information sharing initiatives to ensure that entities have the knowledge and skills necessary to monitor their networks effectively.

- **Partnerships with Managed Security Service Providers (MSSPs):** SLTTs can establish partnerships with MSSPs to monitor, audit, and track network traffic and activity on behalf of entities within their jurisdiction. This can be done through contracts with the MSSPs, who can provide centralized monitoring and reporting capabilities.

- **Cloud-based Security Services:** SLTTs can leverage cloud-based security services to monitor, audit, and track network traffic and activity. This can be done through contracts with cloud service providers, who can provide centralized monitoring and reporting capabilities.

- **Collaborative Monitoring:** SLTTs can establish a collaborative monitoring program that brings together entities within their jurisdiction to share monitoring data and collaborate on threat identification and response. This can be done using a shared platform that enables entities to share data and collaborate on threat identification and response.

  SLTTs are encouraged to leverage established partnerships with agencies such as CISA, MS-ISAC, and/or vendor network monitoring, auditing, and tracking services to enhance their capabilities for monitoring, auditing, and tracking network traffic and activity. By doing so, state and local government can leverage best practices and expertise across the cybersecurity community to enhance Alaska's overall cybersecurity posture. The State of Alaska has partnered with a variety of organizations to bolster its cybersecurity measures. One such partnership is with the Alaska Federation of Natives, which launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills. The state has also partnered with Arctic Slope Regional Corporation and the University of Alaska to establish the Alaska Cybersecurity Center, which offers

training and research opportunities to students and professionals. Additionally, the state has worked with the Department of Homeland Security to conduct cybersecurity risk assessments and develop response plans.

These partnerships demonstrate the State of Alaska's commitment to staying ahead of cyber threats and ensuring that its citizens, businesses, and infrastructure are protected. By collaborating with various organizations, the state can leverage their expertise and resources to create a more secure cyber landscape.

- Network Security: SLTTs can establish a comprehensive network security program that includes all information systems, applications, and user accounts owned or operated by the state or local government entities within the jurisdiction of the state. This program should incorporate best practices and methodologies to ensure that the SLTTs are effectively monitoring, auditing, and tracking vulnerabilities and threats. By doing so, the SLTTs will enhance their cybersecurity resilience and interoperability by ensuring that we are effectively securing our network infrastructure.

The State of Alaska and the SLCGP planning committee will identify and assist with coordinating activities between local government entities and federal partners to enhance network monitoring, auditing, and tracking of network traffic and activity. By leveraging partnerships, cloud-based services, collaborative monitoring programs, and cybersecurity services, the state aims to ensure effective cybersecurity resilience, information sharing, and interoperability across all levels of government. This commitment aligns with our goal to stay ahead of cyber threats and protect the state's citizens, businesses, and infrastructure, and enhance their overall cybersecurity resilience meeting the requirement of SLCGP: e.2.B.iv.

ENHANCE PREPAREDNESS

The State of Alaska will collaborate with relevant agencies and stakeholders to develop and implement a comprehensive cybersecurity preparedness plan that includes all levels of government within the state. The plan will be based on Risk Management Best Practices and Frameworks and will identify and prioritize key resources that are vital to the state's economy, public health, and safety.

We will work with relevant state, local and federal agencies to provide training and exercise support to SLTT organizations to enhance their cybersecurity preparedness. The State of Alaska recommends these activities include tabletop exercises, functional exercises, and full-scale exercises to test and evaluate the state's cybersecurity response capabilities.

Additionally, we will expand ongoing training programs to enhance the knowledge and skills of personnel within the community to address cybersecurity risks and threats. The recommended topics include cybersecurity hygiene training, awareness campaigns, and training on the latest cybersecurity technologies and best practices.

To enhance our response capabilities, we will develop and implement incident response plans and procedures to address cybersecurity incidents promptly and effectively. We will also ensure that our response plans align with the National Incident Management System (NIMS) and the National Response Framework (NRF).

Through these efforts, the State of Alaska will enhance its preparation, response, and resiliency against cybersecurity risks and threats, and promote and support that for SLTTs. As we achieve our program objectives, we will report our progress and outcomes to relevant stakeholders and adjust our strategies as necessary.

Assessment and Mitigation

The State of Alaska's strategic approach to implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk will focus on improving the state's ability to identify and mitigate cybersecurity threats and vulnerabilities on information systems, applications, and user accounts across state and local governments.

To achieve this, the state will encourage, support, and collaborate with local entities to develop comprehensive cybersecurity risk assessments to be performed annually, including identifying potential vulnerabilities and prioritizing mitigation efforts based on the level of risk. The State will also encourage and support the development and implementation of policies and procedures for vulnerability management, including timely application of security patches and updates, regular vulnerability scans, and penetration testing.

The State of Alaska acknowledges the significance of identifying and mitigating cybersecurity threats and vulnerabilities to uphold the ongoing protection of critical information systems, applications, and user accounts. As part of its commitment, the State of Alaska will require, through the grant process, grantees conduct a self-assessment and engage in ongoing follow-ups. This collaborative effort between state and local government entities will establish a continuous process of cybersecurity vulnerability assessments and threat mitigation practices, prioritized based on the degree of risk.

To ensure that local entities have access to the necessary tools and resources, the State will expand ongoing training, cyber incident exercise, and cybersecurity information sharing. By regularly assessing and mitigating cybersecurity threats and vulnerabilities, the State of Alaska will improve the overall cybersecurity posture of state and local government entities and meet the requirement SLCGP: e.2.B.iv.

Best Practices and Methodologies

The State of Alaska recognizes the importance of adopting and using best practices and methodologies to enhance cybersecurity. To improve the overall security posture of SLTT organizations, the following cybersecurity best practices will be encouraged, and eligible for available grant funding, to be implemented within a reasonable timeline according to the prioritization that emerges from the self-assessment:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Identify and implement compensating controls to mitigate threats to unsupported software and hardware
- Prohibit use of known/fixed/default passwords and credentials
- Ensure the ability to reconstitute systems (backups)
- Migrate to the .gov internet domain
- Implement network boundary filtering capabilities where practicable (e.g., DNS, URL, Email)
- Implement [cyber]security awareness training program.

- Implement authentication and privileged account access in alignment with best practices and standards on an annual basis.
- Implement a Patch Management Solution

These best practices will be incorporated statewide and individual projects that assist SLTT entities adopting these best practices will be prioritized.

NIST Principles

In addition to the above best practices, the State of Alaska will adopt recognized frameworks such as NIST Cybersecurity Framework (CSF) or equivalent frameworks to significantly improve its ability to meet cybersecurity requirements. The State of Alaska will work to implement NIST CSF or an equivalent framework as the foundation for its Cybersecurity Program and work towards its widespread adoption among state and local entities.

Supply Chain Risk Management

Supply Chain Risk Management is a critical aspect of cybersecurity, and the State of Alaska will adopt cyber supply chain risk management (C-SCRM) best practices identified by NIST. The state will identify, prioritize, and assess information technology suppliers, vendors, and service providers – including to work with and through local partners - to understand the related and/or cascading risks to the state and local supply chain.

Tools and Tactics

To continuously improve cybersecurity best practices, the State of Alaska will engage with MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics. The State encourages SLTTs to participate in government and cybersecurity conferences and liaise with cybersecurity professionals from federal, state, and private entities to share indicators of compromise, best practices, and threat intelligence. Partnerships with affiliated organizations will enhance the State's ability to share opportunities and information.

Safe Online Services

The State of Alaska is committed to promoting the delivery of safe, recognizable, and trustworthy online services. As part of this effort, the state is encouraging the use of the .gov internet domain for all state agencies and local entities that are eligible for the domain.

To support the adoption of the .gov domain, the state is providing technical assistance and resources to eligible entities. This includes guidance on how to obtain a .gov domain, as well as assistance with domain registration and implementation. Additionally, the state is promoting the use of cybersecurity tools, such as external vulnerability scanning, automated vulnerability monitoring, scanning, and reporting to ensure that online services are safe and secure.

The state is also committed to ongoing education and awareness efforts to promote safe online practices among employees and the public. This includes regular cybersecurity training and awareness campaigns, as well as public outreach initiatives to raise awareness about online risks and best practices for staying safe online.

By promoting the use of the .gov domain and providing resources and support for safe online services, the State of Alaska is demonstrating its commitment to enhancing cybersecurity and ensuring the delivery of safe and trustworthy online services.

Continuity of Operations

Continuity of Operations (COOP) planning is essential to ensure the delivery of critical services and operations in the event of a cyber incident. The State of Alaska will establish a comprehensive COOP program to ensure the continuity of critical services and operations during and after a cyber incident. This program will be developed in coordination with the Alaska Division of Homeland Security and Emergency Management and will include partnerships with local and tribal governments.

The State of Alaska will provide resources to support COOP planning and emergency response efforts. The State will also promote ongoing training and exercises to enhance COOP preparedness and response capabilities.

For this two-year Plan, the State of Alaska will prioritize the development of viable, comprehensive COOP plans and business continuity programs for state agencies, local governments, and tribal entities. The State will collaborate with partners to expand ongoing training, cyber incident exercise, and cybersecurity information sharing, which will support local entities' COOP planning efforts.

The State will also establish performance measures to track the maturity of COOP planning efforts and incident response preparedness. The State of Alaska is committed to ensuring continuity of operations in the face of cyber incidents and demonstrates that the plan meets requirement SLCGP: e.2.B.vii.

Workforce

The State of Alaska is committed to using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as improving personnel's knowledge, skills, and abilities to address cybersecurity risks and threats.

To support this initiative, the State of Alaska will work to build alliances with employers, educational institutions, and public and private partners to develop training and educational pathways to provide the needed skilled workers in the cybersecurity field.

Initiatives will focus on developing internships and apprenticeships, promoting cybersecurity education in K-12 and higher education, and utilizing state-supported internship programs.

The State of Alaska will also provide ongoing training to personnel at all levels in good cyber hygiene and best cybersecurity practices. This will include promoting the adoption of the NICE Framework in state and local hiring practices and encouraging interested individuals to further develop their cybersecurity skills through internships and educational opportunities.

The State will continue to monitor the its cybersecurity workforce and promote the adoption of best practices and the NICE Framework to ensure the State of Alaska has a skilled and effective cybersecurity workforce, meeting requirement SLCGP: e.2.B.viii.

Continuity of Communications and Data Networks

The State of Alaska recognizes the critical need for cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks. To address this need, the State of Alaska will ensure that all entities have access to a comprehensive and regularly

updated Incident Response Plan that provides instructions for communication during an incident and how to handle situations where the secure and preferred communication method is unavailable.

The State of Alaska will ensure that all entities are trained in the use of these communication and data network systems and will conduct regular exercises to test their effectiveness in maintaining continuity of operations. The State of Alaska will also establish procedures for the use of Traffic Light Protocol (TLP) when sharing incident information to ensure that sensitive information is only shared with appropriate audiences.

Through these efforts, the State of Alaska will ensure cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks, meeting requirement SLCGP: e.2.B.ix.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

The State of Alaska Division of Homeland Security and Emergency Management (DHSEM) conducts a federally required Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) every three years. The State recognizes the importance of assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources, such as power and telecommunications, that may impact the performance of information systems within its purview. To accomplish this goal, the state will conduct regular assessments of its capabilities across relevant mission areas, including Prevention, Protection, Mitigation, Response, and Recovery.

Alaska will encourage and support the use of established frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or equivalent, to guide its assessment and mitigation efforts. These assessments target federal and state funding to mitigate cybersecurity risks and threats to critical infrastructure and key resources.

The state will work closely with its partners, including local jurisdictions and private sector organizations, to identify and prioritize critical infrastructure and key resources and develop strategies to enhance their cybersecurity posture. The state will share and promote the adoption of best practices and cybersecurity frameworks, such as the NIST Cybersecurity Framework, to ensure that critical infrastructure and key resources are protected to the greatest degree possible.

Alaska recognizes that assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources is an ongoing process that requires continuous monitoring and improvement. The state will regularly review and update its strategies and plans to ensure that they remain effective and responsive to the evolving threat landscape. These efforts demonstrate that the state is committed to meeting requirement SLCGP: e.2.B.x.

Cyber Threat Indicator Information Sharing

The State of Alaska is committed to enhancing its capacity and capabilities to share cyber threat indicators and related information with relevant stakeholders. To achieve this goal, we will leverage CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems, and other applicable systems and processes.

Additionally, we will encourage all entities to subscribe to and participate in the MS-ISAC Real-Time Indicator Feeds to stay up to date on emerging threats and vulnerabilities. We will also promote the adoption of CISA's free cybersecurity services to local entities through outreach efforts and state and federal partnerships.

As part of our commitment to information-sharing, we will maintain active collaborations with our federal, state, local, tribal (SLTT) partners, as well as organizations like the Alaska Municipal League (AML), to collectively identify and address cybersecurity threats and vulnerabilities. By leveraging these partnerships, we aim to enhance our ability to identify and mitigate potential risks to our critical infrastructure and key resources, thereby ensuring the uninterrupted continuity of our operations even in the face of a cyber incident. This comprehensive plan aligns with and fulfills the requirement SLCGP: e.2.B.xii.

Department Agreements

The State of Alaska is committed to sharing cyber threat indicators and related information with all SLTTs, including expanding information sharing agreements with CISA. Alaska will expand information sharing by working with partners by developing options for centralizing communication and information sharing to share cyber threat information products with federal, and SLTT partners. The SLCGP committee will continue to work towards expanding and evolving the sharing of cyber threat indicators, incidents after action reports, and other related information with CISA and MS-ISAC. As part of Alaska's cybersecurity plan, we will focus on improving and enhancing cybersecurity intelligence and information sharing across all levels of government, including local, regional, state, and federal organizations. Through this plan, we will initiate projects to achieve this goal and expand our capability to share cyber threat indicator information with DHS, meeting requirement SLCGP: e.2.B.xi.I-II.

Leverage CISA Services

The State of Alaska recognizes the importance of leveraging the cybersecurity services offered by CISA to enhance our cybersecurity posture. Alaska currently participates in several CISA programs, including the Automated Indicator Sharing (AIS) and the Cyber Hygiene program.

The Alaska Division of Homeland Security and Emergency Management (DHSEM) will continue to collaborate with CISA to identify opportunities to expand our participation in these programs and explore additional cybersecurity services offered by CISA that could benefit our state.

DHSEM will also work to increase awareness of the benefits of these services among state and local entities and promote adoption of CISA's cybersecurity best practices and guidelines. The State encourages CISA to ensure adequate timeliness and responsiveness to needs especially of SLTTs, including to provide technical assistance as they implement local planning efforts.

Through these efforts, Alaska aims to strengthen our cybersecurity capabilities and meet the requirements of SLCGP: e.2.B.xii.

Information Technology and Operational Technology Modernization Review

The State of Alaska is committed to ensuring alignment between information technology (IT) and operational technology (OT) cybersecurity objectives. As part of this Statewide Alaska Cybersecurity Strategic Plan, we will encourage and support a modernization review process to identify and mitigate cybersecurity risks and threats to IT and OT systems.

The State encourages and supports regular assessments of IT and OT systems to ensure they are properly secured and updated. We will prioritize the implementation of security controls and risk management strategies to address any vulnerabilities identified during these assessments.

To ensure effective alignment between IT and OT cybersecurity objectives, we will encourage and support the creation of a cross-functional team comprising IT and OT professionals from SLTTs who will work collaboratively to identify and mitigate cybersecurity risks and threats. This team will be responsible for

evaluating new technologies and solutions to ensure they are secure and compatible with both IT and OT systems.

We will continue to establish partnerships with industry experts and vendors who specialize in OT cybersecurity to gain valuable insights and expertise in securing critical infrastructure and key resources. These partnerships will help us identify emerging threats and vulnerabilities, as well as best practices for securing IT and OT systems.

Through these efforts, we will ensure that our IT and OT systems are secure and resilient, and that we can effectively respond to and mitigate cybersecurity risks and threats to our critical infrastructure and key resources.

Cybersecurity Risk and Threat Strategies

The SLCGP Committee of the State of Alaska will develop and coordinate strategies to address cybersecurity risks and threats in collaboration with other organizations. This will include consulting with local governments and associations of local governments, neighboring entities, and Tribal governments, or members of an ISAC; and other states. We will establish a process to ensure effective communication and collaboration with relevant entities and organizations. We will participate in the activities of organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) to enhance information sharing and collaboration with other states.

Our approach will involve regular coordination and information sharing with neighboring entities, , and Tribal governments to ensure that we have a comprehensive understanding of cybersecurity risks and threats in our region. We will work with these entities to develop coordinated response plans and strategies to address cybersecurity incidents that affect our jurisdictions.

In addition, we will collaborate with federal agencies such as the Department of Homeland Security and the Federal Bureau of Investigation to enhance our cybersecurity capabilities and ensure effective incident response. The State of Alaska is committed to a proactive and collaborative approach to cybersecurity risk and threat strategies, meeting requirement SLCGP: e.2.B.xiv.

Rural Communities

The State of Alaska recognizes the importance of ensuring that rural communities have adequate access to and can participate in cybersecurity services and activities. As a geographically expansive state, with many rural and remote communities, the state government is committed to providing cybersecurity services and resources to all Alaska public and local entities, regardless of their location or socioeconomic status.

To achieve this goal, the state government will work closely with local governments, associations of local governments, and tribal governments to identify and address any barriers to access that may exist in rural communities. This will involve consultation with these communities to understand their unique needs and challenges related to cybersecurity.

The state government will also help public sector entities explore the use of technology to provide cybersecurity services and resources to rural communities. This may include the use of virtual training and educational materials, as well as remote access to cybersecurity experts and support services.

In addition, the state government will promote public-private partnerships that can help to address the cybersecurity needs of rural communities. This may involve working with local businesses, non-profits, and other organizations to provide cybersecurity training and support to individuals and organizations in rural areas.

Overall, the State of Alaska is committed to ensuring that all Alaska entities, regardless of their location or background, have access to the cybersecurity services and resources they need to protect themselves and their communities from cyber threats.

FUNDING & SERVICES

The State of Alaska plans to utilize grant funding to support its comprehensive cybersecurity plan, including initiatives to improve the cybersecurity practices of state agencies and local entities. The state will distribute funds, items, services, capabilities, or activities to local governments, including plans to distribute at least 25% of cybersecurity grant funding received to rural areas.

In the first year of the program, the State of Alaska will focus on providing cost-effective and scalable cybersecurity services to local governments, including rural communities. These services will include assessments, audits, continuity planning, response planning, exercises, and skill enhancement for local entities. The state will work directly and collaborate with relevant agencies and partners to ensure a comprehensive and multi-faceted approach.

The State of Alaska will also work to expand and evolve cybersecurity practices across state agencies through improving vulnerability management and penetration testing and creating metrics and reports to prioritize remediation action. The state will use NIST 800-53 as a framework for implementing these initiatives.

Distribution to Local Governments

The State of Alaska aims to support local governments through implementing its comprehensive cybersecurity plan and by providing resources that enable delivery of the plan's objectives. These details will be listed in a table found in Appendix B: Project Summary Worksheet. To ensure the successful implementation of the cybersecurity plan, the state will distribute funds, items, services, capabilities, or activities to local governments. Additionally, the state plans to allocate at least 25% of the cybersecurity grant funding received specifically to rural areas.

ASSESS CAPABILITIES

The State of Alaska will adopt a strategic approach to assess the capabilities of entities applying for funding through the grant program for the various cybersecurity plan elements. This approach aims to comprehensively evaluate the cybersecurity capabilities of each entity, specifically addressing the requirements outlined in Appendix A: Cybersecurity Plan Capabilities Assessment. The assessment of Alaska's cybersecurity capabilities will be conducted at different levels, namely Foundational, Fundamental, Intermediate, and Advanced.

To assess these capabilities, the State of Alaska will leverage the NIST Cybersecurity Framework and the NICE Workforce Framework for Cybersecurity. Furthermore, a gap analysis will be conducted to identify areas that require improvement and enhancement in terms of cybersecurity capabilities. The State will support and encourage SLTTs to perform their own gap analysis that can be funded through the grant program.

Based on the assessment outcomes, Alaska will identify areas that necessitate increased capabilities and will develop action plans to address those gaps. Clear assignment of responsibilities to relevant parties and target completion dates will be established for each action plan.

In addition, periodic assessments will be conducted to ensure the continuous effectiveness of Alaska's cybersecurity capabilities in addressing emerging cyber threats and risks. These assessments will follow a regular schedule and involve all relevant stakeholders.

Overall, Alaska remains dedicated to the ongoing enhancement of its cybersecurity capabilities, ensuring effective protection of information systems and critical infrastructure against cyber threats and risks.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

The Department of Administration, under the State of Alaska, takes the lead in managing the executive branch cybersecurity program. Specifically, it oversees the Office of Information Technology (OIT), which is responsible for safeguarding and managing the IT infrastructure of the state's executive branch. The OIT ensures the implementation of cybersecurity policies and standards, and its primary focus is on securing the executive branch's IT systems and infrastructure. The SLCGP Committee, consisting of representatives from various state agencies and levels of government, is responsible for developing and implementing the Statewide Alaska Cybersecurity Strategic Plan. The Committee will coordinate with local governments and associations, neighboring entities, Tribal governments, and ISACs to ensure effective implementation of the Plan.

The following roles and responsibilities have been defined for the implementation of the Statewide Alaska Cybersecurity Strategic Plan:

- The Department of Administration will serve as the lead agency for the cybersecurity program and oversee the implementation of the Plan.
- The OIT will manage and secure the state's IT infrastructure, oversee compliance with cybersecurity policies and standards, and ensure the implementation of the Plan.

The State of Alaska, through its Emergency Management and grant administration, will play a vital role in the development, implementation, and coordination of the comprehensive cybersecurity plan. The SLCGP (State and Local Cyber Grant Program) Committee will take the lead in developing and implementing the plan, ensuring effective coordination with other organizations involved in cybersecurity efforts. Furthermore, the committee will oversee the overall implementation of the plan, working closely with the State of Alaska Emergency Management and grant administration to ensure its successful execution. Each goal and objective in the Plan has a timeline with a target completion date and one or more owners responsible for overseeing and coordinating its completion. Accomplishing the goals and objectives will require support and cooperation from various individuals, groups, or agencies. Regular governance body meetings will include formal agenda items for reviewing the progress of the Plan's implementation.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

The implementation of this comprehensive cybersecurity plan will require collaboration, resources, and investments across the State of Alaska. The resources needed to execute this plan include funding, personnel, and technology.

Funding will be needed to support the implementation of cybersecurity tools and technologies, as well as to develop and execute training and awareness programs. Personnel will be required to support the implementation of the cybersecurity plan, including cybersecurity professionals to conduct risk

assessments, manage cybersecurity tools, and provide training to personnel. Technology investments will be necessary to enhance the security posture of the state's information systems and networks.

The timeline for implementing the cybersecurity plan is as follows, for the State, with corresponding support for local governments and Tribes to align their efforts to this schedule:

- Year 1: Conduct a comprehensive risk assessment of the state's information systems and networks, identify critical infrastructure, and key resources, and develop a cybersecurity training and awareness program for state personnel.
- Year 2: Implement additional cybersecurity tools and technologies, including endpoint protections, data loss prevention, and multifactor authentication. Continue to expand the use of the .gov domain and cybersecurity tools to boroughs and cities. Grantees can apply for funding to implement these tools.
- Year 3: Develop and implement a continuity of operations plan for cybersecurity incidents and conduct regular exercises to test the plan. Expand ongoing training, cyber incident exercises, and cybersecurity information sharing to support local entities.
- Year 4: Focus on workforce development, using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the state's cybersecurity workforce. Continue to leverage CISA services and expand information sharing agreements with local governments. Conduct a review of information technology and operational technology modernization to ensure alignment between cybersecurity objectives.
- Year 5: Develop and coordinate strategies to address cybersecurity risks and threats with other organizations, including consultation with local governments, neighboring entities, territories, and tribal governments. Ensure rural communities have adequate access to and can participate in cybersecurity services and activities.

These timelines are subject to change based on the availability of resources and other factors that may impact the state's ability to implement this comprehensive cybersecurity plan. The State of Alaska will regularly review and update this plan to ensure its effectiveness and relevance to the current cybersecurity landscape.

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY PLANNING COMMITTEE				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts	State agencies and some local jurisdictions currently manage, monitor, and track varying levels of information systems, applications, and user accounts	Foundational		
2. Monitor, audit, and track network traffic and activity	State agencies and some local jurisdictions currently monitor, audit, and track network traffic and activity	Foundational		
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	State agencies and some local jurisdictions engage in practices to enhance preparation, response, and resiliency	Foundational	1	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	State agencies and some local jurisdictions engage in regular cybersecurity assessments and risk	Foundational	2	

	management activities			
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	State agencies and some local jurisdictions implement the best practices listed in Plan Element 5	Foundational		
a. Implement multi-factor authentication	State agencies and some local jurisdictions implement MFA	Foundational		
b. Implement enhanced logging	State agencies and some local jurisdictions implement enhanced logging	Foundational		
c. Data encryption for data at rest and in transit	State agencies and some local jurisdictions utilize encryption for data at rest and in transit	Foundational		
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	State agencies and some local jurisdictions exercise life cycle management practices to end use of unsupported/end of life software and hardware	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	State agencies and some local jurisdictions prohibit use of known/fixed/default password and credentials	Foundational		

f. Ensure the ability to reconstitute systems (backups)	State agencies and some local jurisdictions ensure the ability to reconstitute critical systems	Foundational		
g. Migration to the .gov internet domain	State agencies and some local jurisdictions have or plan to migrate to .gov	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	State agencies and some local jurisdictions promote the delivery of safe, recognizable and trustworthy online services	Foundational		
7. Ensure continuity of operations including by conducting exercises	State agencies and some local jurisdictions conduct exercises	Foundational		
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	State agencies and some local jurisdictions identify and mitigate any gaps in the cybersecurity workforces	Foundational		
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	State agencies and some local jurisdictions ensure continuity of communications and data networks	Foundational		
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the	State agencies and some local jurisdictions assess and mitigate cybersecurity risks	Foundational	2	

performance of information systems within the jurisdiction of the eligible entity	and threats to critical infrastructure			
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	State agencies and some local jurisdictions enhance capabilities to share cyber threat indicators and information	Foundational		
12. Leverage cybersecurity services offered by the Department	State agencies and some local jurisdictions leverage cybersecurity services offered by the Department	Foundational		
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	State agencies and some local jurisdictions implement modernization cybersecurity review process	Foundational		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	State agencies and some local jurisdictions develop and coordinate strategies to address cybersecurity strategies and risks	Foundational		
15. Ensure rural communities have adequate access to, and participation in plan activities	State agencies and some local rural jurisdictions have adequate access to and participation in plan activities	Foundational		
16. Distribute funds, items, services, capabilities, or activities to local governments	State agencies are prepared to distribute grant funds and some services appropriately	Foundational	1	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

1. Rank	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
1	Statewide Cybersecurity Plan Refinement	Additional planning by Cybersecurity Planning Committee to refine the cybersecurity plan submission for FY2023	1, 2, 3, 4, 5, 6, 10, 12, 13, 14, 15, 16	$20K (TBD)	Ongoing	High	Plan
2	Direct pass-through funds to eligible local government entities based on strength of application, demonstrated need, rural designation, and evidence of ability to sustain investment	Applications will be prioritized based on following identified cybersecurity components: - Conduct vulnerability assessments - Implement multi-factor authentication - Implement enhanced logging - Data encryption for data at rest and in transit - End use of unsupported / end of life software and hardware that are accessible from the internet - Prohibit use of known/fixed/default passwords and credentials -Ensure ability to reconstitute systems (backups)	1, 2, 3, 4, 5, 6, 8, 10, 12, 13, 14, 15, 16	$XXM (TBD)	Future	High	Equip

APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics		
Cybersecurity Plan Metrics		
Goal	**Step**	**Key Performance Indicator**
1. Enhance Cybersecurity Resilience and Interoperability by developing and implementing a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies.	• Develop a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies. • Develop and implement a security awareness training program	• Number of cybersecurity risk assessments conducted annually. • Percentage of vulnerabilities remediated within a defined timeframe. • Compliance with relevant cybersecurity regulations and standards
2. Foster a Cybersecurity Culture by developing and delivering cybersecurity awareness and training programs to state employees, contractors, and local government personnel.	• Develop and deliver cybersecurity awareness and training programs to state employees, contractors, and local government personnel. • Develop and implement a security awareness campaign to increase awareness and promote best practices	• Number of training sessions conducted. • Percentage of employees completing the training • Number of reported security incidents related to employee behavior

Cybersecurity Plan Metrics		
Goal	**Step**	**Key Performance Indicator**
3. Enhance Cybersecurity Collaboration and Partnerships by developing and implementing a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations.	• Develop and implement a cybersecurity information sharing program with local governments, neighboring states, and federal agencies. • Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations	• Number of cybersecurity risk assessments conducted annually. • Percentage of vulnerabilities remediated within a defined timeframe. • Compliance with relevant cybersecurity regulations and standards
4. Improve Cyber Incident Management and Response Capabilities by developing and implementing a cybersecurity incident management plan that is tested and updated on a regular basis and establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents.	• Develop and implement a cybersecurity incident management plan that is tested and updated on a regular basis. • Establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents. • Conduct regular cybersecurity incident response exercises and drills	• Number of cybersecurity incident response exercises conducted annually. • Percentage of incidents handled within defined timeframes. • Effectiveness of incident response team in mitigating the impact of cybersecurity incidents.

APPENDIX D: ACRONYMS

Acronym	Definition
ISAC	Information Sharing and Analysis Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
SLCGP	State and Local Cybersecurity Grant Program
IT	Information Technology
SOC	Security Operations Center
ITOC	Information Technology Operations Center
MSSP	Managed Security Service Provider
CISA	Cybersecurity and Infrastructure Security Agency
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
C-SCRM	Cyber Supply Chain Risk Management
COOP	Continuity of Operations
DHSEM	Division of Homeland Security and Emergency Management
THIRA	Threat and Hazard Identification and Risk Assessment
SPR	Security and Privacy Requirements
CIMS	Cyber Incident Management System
TLP	Traffic Light Protocol
CISCP	Certified Information Systems Cybersecurity Professional
AIS	Automated Information System
SLTT	State, Local, Tribal, and Territorial

APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES

All recipients and subrecipients of the Statewide Alaska Cybersecurity Grant Program (SLCGP) are required to participate in the following free services provided by the Cybersecurity and Infrastructure Security Agency (CISA). Please note that participation in these services is not mandatory for grant submission and approval but is a post-award requirement.

REQUIRED SERVICES AND MEMBERSHIPS

Cyber Hygiene Services:

- **Web Application Scanning:** A service that assesses the health of publicly accessible web applications, identifies vulnerabilities, and recommends security enhancements.
- **Vulnerability Scanning:** Continuous scanning of public, static IPs for accessible services and vulnerabilities, providing weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP." In the body of your email, mention that you are requesting these services as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR):

The NCSR is an annual self-assessment that measures the cybersecurity programs' gaps and capabilities of state, local, and tribal (SLT) entities. It is based on the National Institute of Standards and Technology Cybersecurity Framework and sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Entities and subrecipients should complete the NCSR annually.

For more information, visit the Nationwide Cybersecurity Review (NCSR) website (cisecurity.org).

ENCOURAGED SERVICES, MEMBERSHIPS, AND RESOURCES

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):

Recipients and subrecipients are strongly encouraged to become members of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC: DHS-designated cybersecurity ISAC for SLT governments, providing services and information sharing to enhance their cybersecurity capabilities.

The EI-ISAC: Focuses on election infrastructure cybersecurity, offering cyber defense tools, threat intelligence products, incident response and forensics, cybersecurity awareness, and training.

To register, please visit the MS-ISAC registration page or the EI-ISAC registration page. For more information, visit MS-ISAC (cisecurity.org) and Election Infrastructure Security (cisa.gov).

CISA Recommended Resources, Assessments, and Memberships (not mandatory):

The following resources, assessments, and memberships are recommended by CISA:

- Cyber Resource Hub
- Ransomware Guide (Sept. 2020)
- Ransomware Readiness Assessment (RRA)
- Cyber Security Evaluation Tool (CSET)
- Malicious Domain Blocking and Reporting
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- CISA Services Catalog
- Free Public and Private Sector Cybersecurity Tools and Services

For reporting a cybersecurity incident, visit CISA Central at us-cert.gov/report. For additional CISA services, refer to the CISA Services Catalog. Information on memberships can be found at the Information Sharing and Analysis Organization Standards Organization.

Note: The inclusion of optional resources and memberships in this appendix does not imply mandatory participation but is provided for informational purposes and to support the enhancement of cybersecurity capabilities.

APPENDIX F: KEY TERMS AND DEFINITIONS

Alaska Cybersecurity Center: An organization established in partnership with the Alaska Federation of Natives and the University of Alaska to provide training and research opportunities in cybersecurity.

Alaska Federation of Natives: A partner organization that launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills.

Alaska Native Cybersecurity Enhancement Project: A collaborative initiative aimed at providing cybersecurity training to Alaska Natives.

Automated Indicator Sharing (AIS): A capability provided by the Cybersecurity and Infrastructure Security Agency (CISA) that allows for the automated exchange of cyber threat indicators.

Cloud-based Security Services: Security services and tools offered by cloud service providers (CSPs) to protect and monitor network infrastructure and data stored in cloud environments.

Collaborative Monitoring: A cooperative approach where multiple entities within a jurisdiction share resources, data, and expertise to collectively monitor and respond to cybersecurity threats.

Continuity of Operations (COOP) Planning: Efforts to ensure the continuity of critical services and operations in the event of a cybersecurity incident.

Continuity of Operations Plan (COOP): A plan outlining actions and procedures to be taken during and after a cybersecurity incident to ensure the continuity of critical operations.

Cross-Functional Team: A team comprising professionals from different disciplines or areas of expertise working together to achieve a common cybersecurity goal.

Cyber Incident Exercise: Simulated exercises designed to test the response and resilience of entities in handling cybersecurity incidents.

Cyber Information Sharing and Collaboration Program (CISCP): A program operated by the Cybersecurity and Infrastructure Security Agency (CISA) that facilitates information sharing and collaboration among cybersecurity stakeholders.

Cybersecurity Services: Services provided by specialized organizations or agencies to support the prevention, detection, response, and recovery from cybersecurity incidents.

Data Encryption: The process of converting data into a coded form to prevent unauthorized access, ensuring its confidentiality and integrity.

Data Loss Prevention (DLP): Measures and technologies implemented to prevent the unauthorized disclosure or loss of sensitive data.

Endpoint Protections: Security measures and tools implemented on endpoints (e.g., computers, laptops, mobile devices) to protect against cyber threats.

Funding Prioritization: The allocation of resources and funding based on prioritized cybersecurity risks and threats.

Gap Analysis: The process of identifying gaps or deficiencies in cybersecurity capabilities and developing plans to address them.

Governance Body: A formal body responsible for overseeing the implementation and progress of the cybersecurity plan.

Information Sharing: The process of exchanging relevant and actionable information between organizations or entities to enhance situational awareness, threat detection, and incident response capabilities.

Information Sharing Agreements: Formal agreements established to facilitate the sharing of cyber threat indicators and related information with local governments and other stakeholders.

Local Government: The governing body responsible for the administration and governance of specific local jurisdictions within a state, such as counties, cities, towns, or municipalities.

Managed Security Service Providers (MSSPs): Companies or organizations that offer outsourced cybersecurity services to assist in monitoring, managing, and enhancing an organization's security posture.

Mitigation: Actions taken to reduce the impact of cybersecurity incidents and vulnerabilities.

Modernization Review Process: A systematic assessment of IT and OT systems to identify and mitigate cybersecurity risks and threats.

Monitoring: The process of observing and collecting data or information to track the performance, behavior, or status of a system, network, or activity.

Multi-State Information Sharing and Analysis Center (MS-ISAC): An organization that facilitates the sharing of cyber threat information and collaboration among states.

Multifactor Authentication: A security mechanism that requires the use of multiple factors (e.g., password, biometric, token) for user authentication.

National Initiative for Cybersecurity Education (NICE) Workforce Framework: A framework used to categorize and describe cybersecurity work roles and required competencies.

Network Activity: Actions and interactions occurring within a computer network.

Network Traffic: The flow of data packets transmitted over a computer network.

NIST 800-53: A set of security and privacy controls published by the National Institute of Standards and Technology (NIST) for federal information systems and organizations.

Prevention: Activities and measures aimed at preventing cybersecurity incidents and mitigating potential risks.

Protection: Measures implemented to safeguard critical infrastructure and key resources from cybersecurity threats.

Public-Private Partnerships: Collaborative efforts between public and private sector organizations to address cybersecurity challenges and share resources.

Real-Time Indicator Feeds: Timely and up-to-date information feeds containing indicators of emerging cyber threats and vulnerabilities.

Recovery: Activities undertaken to restore and recover systems and operations following a cybersecurity incident.

Response: Coordinated efforts to address and mitigate the effects of cybersecurity incidents when they occur.

Risk Assessment: The process of identifying, analyzing, and evaluating potential risks and vulnerabilities to determine their potential impact and likelihood.

Security Patches and Updates: Software updates or fixes released by vendors to address identified vulnerabilities and enhance system security.

Self-Assessment: An evaluation conducted by grantees themselves to assess their own cybersecurity preparedness and identify areas for improvement.

SLTTs (State, Local, Tribal, and Territorial): Refers to the collective entities comprising state governments, local governments, tribal governments, and territorial governments.

Stakeholder Preparedness Review (SPR): A federally required review conducted every three years to assess the preparedness of stakeholders in addressing threats and hazards.

Territorial Government: The governing body responsible for the administration and governance of a specific territory or territorial possessions under the jurisdiction of a country.

Threat and Hazard Identification and Risk Assessment (THIRA): A federally required assessment conducted every three years to identify and evaluate threats, hazards, and risks.

Threat Mitigation Practices: Measures and actions taken to reduce or eliminate cybersecurity risks and threats.

Traffic Light Protocol (TLP): A framework used to classify and control the dissemination of sensitive incident-related information.

Tracking: The process of tracing and recording the movement or progress of something.

Tribal Government: The governing body responsible for the administration and governance of Native American tribes or indigenous communities within a country.

Vulnerability Management: The process of identifying, assessing, and addressing vulnerabilities in information systems, applications, and user accounts.

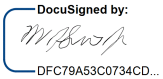
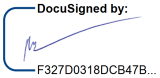
DocuSign

Certificate Of Completion

Envelope Id: E85C5188711042D281F52623E8DDFF10
Status: Completed
Subject: Complete with DocuSign: SoA SLCGP Cybersecurity Plan (Final Draft).docx
Source Envelope:
Document Pages: 34
Signatures: 2
Envelope Originator:
Certificate Pages: 4
Initials: 0
Bill Smith
AutoNav: Enabled
PO Box 110206
EnvelopeId Stamping: Disabled
Juneau, AK 99811
Time Zone: (UTC-09:00) Alaska
bill.smith@alaska.gov
IP Address: 158.145.14.25

Record Tracking

Status: Original
8/10/2023 2:48:48 PM
Holder: Bill Smith
bill.smith@alaska.gov
Location: DocuSign
Security Appliance Status: Connected
Pool: StateLocal
Storage Appliance Status: Connected
Pool: State of Alaska
Location: DocuSign

Signer Events	Signature	Timestamp
Bill Smith bill.smith@alaska.gov CIO State of Alaska Office of Information Technology Security Level: Email, Account Authentication (None)	DocuSigned by:  DFC79A53C0734CD... Signature Adoption: Uploaded Signature Image Using IP Address: 10.2.15.7	Sent: 8/10/2023 2:50:34 PM Viewed: 8/10/2023 2:50:44 PM Signed: 8/10/2023 2:50:55 PM
Electronic Record and Signature Disclosure: Accepted: 3/9/2022 11:45:27 AM ID: bc6ab434-c70f-461d-9daf-26bbb2fbe1a5 Company Name: State of Alaska		
Bryan J Fisher b.fisher@alaska.gov Security Level: Email, Account Authentication (None)	DocuSigned by:  F327D0318DCB47B... Signature Adoption: Uploaded Signature Image Using IP Address: 158.145.14.24	Sent: 8/10/2023 2:50:56 PM Viewed: 8/10/2023 3:19:23 PM Signed: 8/10/2023 3:19:53 PM
Electronic Record and Signature Disclosure: Accepted: 8/10/2023 3:19:23 PM ID: 1a8da33d-2794-4ad4-bac5-a356a3c0f9f6 Company Name: State of Alaska		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Bill Dennis bill.dennis@alaska.gov Administrative Operations Manager Security Level: Email, Account Authentication (None)	COPIED	Sent: 8/10/2023 3:19:55 PM

Carbon Copy Events	Status	Timestamp

Electronic Record and Signature Disclosure:
Accepted: 5/24/2021 7:33:16 AM
ID: 41c94d05-9122-462a-bc2a-1005b430e143
Company Name: State of Alaska

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/10/2023 2:50:34 PM
Certified Delivered	Security Checked	8/10/2023 3:19:23 PM
Signing Complete	Security Checked	8/10/2023 3:19:53 PM
Completed	Security Checked	8/10/2023 3:19:55 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

Please read this Electronic Records and Signature Disclosure (ERSD). It concerns your rights regarding electronically undertaking, and the conditions under which you and the State of Alaska agree to electronically undertake, the transaction to which it relates (the "TRANSACTION").

Consent to Electronically Undertake the TRANSACTION

You can electronically undertake the TRANSACTION only if you confirm that you meet the following requirements by selecting the box next to "I agree to use electronic records and signature" (the "AGREE BOX"):

1. you can fully access and have read this ERSD;
2. you can fully access all of the information in the other TRANSACTION records;
3. you can retain all of the TRANSACTION records in a form that you will be able to fully access for later reference;
4. you consent to undertake the TRANSACTION electronically; and
5. you are authorized to undertake the TRANSACTION. (Please note that falsely undertaking the TRANSACTION may subject you to civil liabilities and penalties and/or to criminal penalties.)

If you cannot or are not willing to confirm each of these five things, do not select the AGREE BOX.

Withdrawing Consent

If you select the AGREE BOX, you can withdraw your consent to electronically undertake the TRANSACTION at any time before you complete the TRANSACTION: simply do not finalize it. The only consequence of withdrawing your consent is that you will not finalize the TRANSACTION.

If you select the AGREE BOX, your consent will apply only to this TRANSACTION. You must separately consent to electronically undertake any other transaction with the State of Alaska.

Paper Option for Undertaking the TRANSACTION

You may undertake the TRANSACTION with the State of Alaska using paper records. (State of Alaska employees who want to undertake the TRANSACTION in paper should contact the agency responsible for the TRANSACTION.) Print the paper records on the website of the State of Alaska agency responsible for the TRANSACTION, or request them from the agency. The State of Alaska homepage is at http://alaska.gov/.

Copies of TRANSACTION Records

After completing the TRANSACTION but before closing your web browser, you should download the TRANSACTION records. Or you can download the records within 30 days after

completing the TRANSACTION using the link in the DocuSign email sent to the email address you used to complete the TRANSACTION. The State of Alaska will not provide a paper copy of the TRANSACTION records as part of the TRANSACTION. Under the Alaska Public Records Act (APRA), AS 40.25.100–.295, you can request a copy from the agency responsible for the TRANSACTION, but if too much time has passed, the agency may no longer have the records when you make your request. If required under the APRA, the agency will charge a fee.

Required Hardware and Software

For the minimum system requirements to electronically undertake the TRANSACTION, including accessing and thereby retaining the TRANSACTION records, visit https://support.docusign.com/guides/signer-guide-signing-system-requirements. These requirements may change. In addition, you need access to an email account.

How to Contact the State of Alaska

To ask a question on this ERSD or the DocuSign document generated after you complete the TRANSACTION or on using DocuSign to electronically undertake the TRANSACTION, contact the Alaska Department of Administration at either of the following addresses:

State of Alaska
Department of Administration
550 West 7th Avenue
Suite 1970
Anchorage, AK 99501
Reference: DocuSign

doa.commissioner@alaska.gov
Subject: DocuSign

To ask any other question on the TRANSACTION records or to update the information for contacting you electronically, contact the State of Alaska agency responsible for the TRANSACTION using the contact information in the TRANSACTION records or, if those records contain no contact information, using the contact information on the agency's website. Again, the State of Alaska homepage is at http://alaska.gov/.