TILLAMOOK COUNTY
BOARD OF COMMISSIONERS
Mary Faith Bell – Doug Olson – Erin Skaar

BOARD MEETING
Wednesday, January 3, 2024, 9:00 AM

Join In Person:
County Courthouse, Board of Commissioners' Meeting Room 106, 201 Laurel Avenue, Tillamook

Join Virtually:
tillamookcounty.gov/bocc/page/meetings-agendas-minutes or 1-971-254-3149, Conference ID: 866 914 607#

Additional viewing options are available at tctvonline.com. Closed captioning and translation options are available for recorded videos at *www.youtube.com/@tillamookcounty1434*.

More detailed meeting instructions are available at *tillamookcounty.gov/bocc/page/meetings-agendas-minutes*. Call 503-842-1814 or send an email to helpdesk@tillamookcounty.gov regarding any meeting technical issues.

CALL TO ORDER

1. Welcome & Request to Sign Guest List
2. Pledge of Allegiance
3. Public Comment
4. Non-Agenda Items

LEGISLATIVE - ADMINISTRATIVE

5. Consideration of a Criminal Justice Commission Justice Reinvestment Program JRP-23-26 Grant Agreement/Lieutenant Ahnie Seaholm, Sheriff's Office
6. Consideration of a Fifth Amendment to Oregon Health Authority Agreement #180028 2023-2025 Intergovernmental Agreement for the Financing of Public Health Services/Marlene Putman, Administrator, Health and Human Services
7. Consideration of Amendment #2 to Contract for Services #6298 with Clair Company, Inc. for Inspection Services/Sarah Absher, Director, Department of Community Development

AGENDAS

COMMUNITY UPDATE – 2024-01-02 COMMUNITY UPDATE AUDIO.MP4

CALL TO ORDER: Tuesday, January 2, 2024 8:01 a.m.

1.	00:40	Welcome and Board of Commissioners' Roll Call
2.	01:23	Adventist Health Tillamook
3.	02:37	Coastal Caucus
4.	10:55	Nehalem Bay Health Center & Pharmacy
5.	11:27	Tillamook Family Counseling Center
6.	12:33	Sheriff's Office
7.	14:06	Emergency Management
8.	28:49	Oregon Department of Transportation
		AGENDA ITEM TAKEN OUT OF ORDER
9.		Board of Commissioners
	22:26	Commissioner Bell
	36:11	Commissioner Olson Joined the Meeting
10.		Cities
	19:41	Rockaway Beach
	20:08	Garibaldi
	20:45	Bay City

ADJOURN – 8:41 a.m.

MEETING – 2024-01-03 BOCC MEETING AUDIO.MP4

CALL TO ORDER – 9:04 a.m.

1.	00:40	Welcome & Request to Sign Guest List
2.	02:41	Pledge of Allegiance
3.	-------	Public Comment: There were none.
4.	03:05	Non-Agenda Items: Item #11 Postponed, Unscheduled Agenda Item After #13/Commissioner Mary Faith Bell

LEGISLATIVE - ADMINISTRATIVE

5. 03:52 Consideration of a Criminal Justice Commission Justice Reinvestment Program JRP-23-26 Grant Agreement/Lieutenant Ahnie Seaholm, Sheriff's Office

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Chair signed the grant agreement.

6. 11:16 Consideration of a Fifth Amendment to Oregon Health Authority Agreement #180028 2023-2025 Intergovernmental Agreement for the Financing of Public Health Services/Commissioner Erin Skaar

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Chair signed the amendment.

7. 12:56 Consideration of Amendment #2 to Contract for Services #6298 with Clair Company, Inc.for Inspection Services/Sarah Absher, Director, Department of Community Development

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Chair signed the amendment.

8. 15:48 Consideration of an Order in the Matter of the Reappointment of a Member to the Tillamook County Housing Commission/Parker Sammons, Housing Coordinator, Department of Community Development

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Board signed Order #24-001.

9. 19:09 Consideration of a Letter of Support to the Oregon Office of Emergency Management for a State and Local Cybersecurity Grant Program Project Application/Jeff Underwood, Manager, Information Services

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Board signed the letter of support.

10. 24:23 Consideration of an Out-of-State Travel Authorization for Commissioner Erin Skaar to Attend the National Association of Counties Legislative Conference in Washington, D.C., 2/9 - 2/14/2024/Commissioner Erin Skaar

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Chair signed the travel authorization.

11. ------ Consideration of Modification #2 to Personal Services Agreement #6374 with DLR Group Architecture & Planning Inc. for the District Attorney's Office Remodel Project/Rachel Hagerty, Chief of Staff

AGENDA ITEM POSTPONED

12. 31:00 Consideration of an Intergovernmental Agreement with Tillamook County Transportation District for Financial Support of Transit Services Operations/Rachel Hagerty, Chief of Staff

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Chair signed the agreement.

13. 34:58 Consideration of an Order in the Matter of the Reappointment of a Member to the Tillamook County Library Board/Don Allgeier, Library Director

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Board signed Order #24-002.

39:02 **UNSCHEDULED:** Consideration of Approval for the Tillamook County Library Closure on January 20, 2024/Don Allgeier, Library Director

A motion was made by Commissioner Skaar and seconded by Vice-Chair Olson. The motion passed with three aye votes. The Board approved the closure.

14. Board Concerns:
46:19 Sandlake Road Update/Commissioner Doug Olson
56:23 Governor's Emergency Declaration/Commissioner Erin Skaar
56:51 Emergency Funding for Weather-Related Damage/Commissioner Mary Faith Bell

15. 59:21 Board Announcements

ADJOURN – 10:05 a.m.

8. Consideration of an Order in the Matter of the Reappointment of a Member to the Tillamook County Housing Commission/Parker Sammons, Housing Coordinator, Department of Community Development

9. Consideration of a State and Local Cybersecurity Grant Program Project Application/Jeff Underwood, Manager, Information Services

10. Consideration of an Out-of-State Travel Authorization for Commissioner Erin Skaar to Attend the National Association of Counties Legislative Conference in Washington, D.C., 2/9 - 2/14/2024/Commissioner Erin Skaar

11. Consideration of Modification #2 to Personal Services Agreement #6374 with DLR Group Architecture & Planning Inc. for the District Attorney's Office Remodel Project/Rachel Hagerty, Chief of Staff

12. Consideration of an Intergovernmental Agreement with Tillamook County Transportation District for Financial Support of Transit Services Operations/Rachel Hagerty, Chief of Staff

13. Consideration of an Order in the Matter of the Reappointment of a Member to the Tillamook County Library Board/Don Allgeier, Library Director

14. Board Concerns - Non-Agenda Items

OTHER MEETINGS AND ANNOUNCEMENTS

The Board of Commissioners' Office is excited to announce the December 29, 2023 launch of the commissioners' new agenda and meeting management system, CivicClerk. CivicClerk is an online platform that streamlines meeting workflow, creating, managing, and archiving agendas, minutes, and audio/video.

We will have a new meeting webpage on the commissioners' site that will function as a portal where all meeting information is easily searchable and accessible. Throughout January, a shortcut on the county's home page at tillamookcounty.gov will aid in navigating to the new meeting webpage.

Our meetings will continue to be livestreamed, and starting December 29, you can join us by going online to tillamookcounty.gov/bocc/page/meetings-agendas-minutes. The teleconference number is 1-971-254-3149, Conference ID: 866 914 607#.

New Year's Day is an observed holiday for Tillamook County. All County offices in the courthouse will be CLOSED on Monday, January 1, 2024. In addition, the Tillamook County Library, administrative offices in the Jail and Justice Facility, Public Works Department, Community Development Department, Surveyor's Office, and the Health and Human Services Department and clinics will be closed. The State Circuit Court, located in the County Courthouse, will also be CLOSED on Monday, January 1, 2024.

The Commissioners will hold a Board Briefing on Wednesday, January 3, 2024 at 2:00 p.m. to discuss weekly Commissioner updates. The meeting will be held in the Board of Commissioners' Meeting Room 106 in the Tillamook County Courthouse, 201 Laurel Avenue, Tillamook, Oregon. You can join us by going online to tillamookcounty.gov/bocc/page/meetings-agendas-minutes. The teleconference number is 1-971-254-3149, Conference ID: 866 914 607#.

The Commissioners will hold a continuation of a public hearing concerning the dissolving of Beaver Water District on January 17, 2024 at 10:00 a.m. The public hearing will be held in the Board of Commissioners' Meeting Room 106 in the Tillamook County Courthouse, 201 Laurel Avenue, Tillamook Oregon. You can join us by going online to tillamookcounty.gov/bocc/page/meetings-agendas-minutes. The teleconference number is 1-971-254-3149, Conference ID: 866 914 607#.

ADJOURN

BOARD OF COMMISSIONERS' BOARD MEETING

Wednesday, January 3, 2024

	Present	Absent		Present	Absent
Mary Faith Bell	✓		Rachel Hagerty	✓	
Doug Olson	✓		Bill Sargent	✓	
Erin Skaar	✓				

PLEASE PRINT

Name	Email or Address	Item of Interest
Will Chappell		

(Please use reverse if necessary)

TILLAMOOK COUNTY BOARD OF COMMISSIONERS' MEETING

WEDNESDAY, JANUARY 3, 2024

PUBLIC COMMENT SIGN-IN SHEET

PLEASE PRINT

NAME	AREA OF RESIDENCE	NAME OF ORGANIZATION (IF ANY)	AGENDA ITEM
There were no sign-ins			

Tillamook County Board of Commissioners
201 Laurel Avenue, Tillamook, OR 97141
Phone: 503-842-3403

Mary Faith Bell, Chair
Doug Olson, Vice-Chair
Erin D. Skaar, Commissioner

January 3, 2024

Re: Oregon Office of Emergency Management State and Local Cybersecurity Grant Program

We are writing on behalf of Tillamook County to express our strong support for the county's application for funding through the Oregon Office of Emergency Management State and Local Cybersecurity Grant Program. We are seeking financial assistance to conduct a remote penetration test, which is essential for enhancing our county's cybersecurity measures.

Tillamook County is committed to ensuring the security and resilience of our critical information systems and infrastructure. We recognize the ever-growing threat of cyberattacks and the potential consequences they can have on our residents, businesses, and local government operations. The proposed remote penetration test, with an estimated cost of $24,700, is a crucial component of the county's cybersecurity strategy. It will provide the county with a comprehensive assessment of their network and information systems, helping identify vulnerabilities and potential risks. This proactive approach will enable the county to take necessary measures to safeguard our data and infrastructure from cyber threats.

The penetration test will include detailed reconnaissance, vulnerability analyses, and exploitation assessment, all of which are critical steps in understanding our network's security posture and improving our overall security resilience. The outcomes of this test will be documented in a comprehensive report, including identified vulnerabilities, recommendations for mitigation, and proof of concept for exploited findings. By investing in this cybersecurity assessment, we aim to:

1. Strengthen our county's ability to defend against cyber threats.
2. Enhance the protection of sensitive data, particularly related to the well-being of our residents.
3. Improve the overall cybersecurity posture of our local government.

We understand the importance of this grant program in supporting local efforts to enhance cybersecurity. Therefore, we kindly request your consideration of our funding request to undertake this critical initiative. Your support will not only benefit Tillamook County but also contribute to the broader cybersecurity resilience of the state of Oregon.

Thank you for considering our application. We believe that this investment in cybersecurity is a wise step to protect the interests of our community, and we look forward to the opportunity to make a positive impact. If you require any additional information or have any questions regarding our proposal, please do not hesitate to contact our office.

Sincerely,

BOARD OF COMMISSIONERS FOR TILLAMOOK COUNTY, OREGON

MF Bell
Mary Faith Bell, Chair

Doug Olson
Doug Olson, Vice-Chair

Erin Skaar
Erin D. Skaar, Commissioner

2023 State Homeland Security Grant Program

Combined Coversheet

Combine all sub-applicant requests within your county or tribe on this coversheet

Type of Grant Funding: Competitive Award

County or Tribe: _ Tillamook County

Name of Primary Point of Contact for this application packet: __Jeff Underwood

Primary Phone Number: 503 842-3406 x3478 Secondary Phone Number Click here to enter text.

Email: _ jeff.underwood@tillamookcounty.gov

Total Funds Requested: $_ 24,700

Sub-Applicant Information:

Please provide agency name, total funds requested and a brief description of the project (20 words or less).

Example:
Agency Name:___*Anytown Fire Department*_____ Total Funding Request: *$__$30,000*_____
Name of Project: (5 words or less)___*EOP Update*_____

1 Agency Name:_ Tillamook County Total Funding Request: $__ 24,700 _
Name of Project: (5 words or less)_ Tillamook County Cybesecurity Assessment _____

2 Agency Name:_ Click here to enter text. Total Funding Request: $__ Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

3 Agency Name:_ Click here to enter text. Total Funding Request: $__ Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

4 Agency Name:_ Click here to enter text. Total Funding Request: $__ Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

5 Agency Name:_ Click here to enter text. **Total Funding Request: $__** Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

6 Agency Name:_ Click here to enter text. **Total Funding Request: $__** Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

7 Agency Name:_ Click here to enter text. **Total Funding Request: $__** Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

8 Agency Name:_ Click here to enter text. **Total Funding Request: $__** Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

9 Agency Name:_ Click here to enter text. **Total Funding Request: $__** Click here to enter text. _
Name of Project: (5 words or less)_ Click here to enter text. _____

***Denotes a regional project**

This Document does not need to be signed. Please submit it as a word document, not a PDF.

If you have any questions, please Contact the SHSP grant Coordinator, Kevin Jeffries.
Kevin.jeffries@oem.oregon.gov or call 971-719-0740

FY22 SLCGP Sub-applicant Coversheet "Pre-Registration Form"

Please use this form to complete your Sub-Applicant Coversheet. **Before you click submit**, you will need to right click on your mouse and select **Print** to print and save a copy. You will need to submit this save form with your application in Basecamp.

* Required

1. Name of Applicant Agency *

   Tillamook County

2. Official name of agency seeking funds (City, Tribe, County, Special District etc.) This name needs to match the one associated with your UE-ID number. *

   County of Tillamook

3. Is the Applicant Agency considered rural as defined in the Notice of Funding Opportunity? From a county with a population of less than 50,000, or a city from within a county with a population of less than 50,000. *

   - (●) Yes
   - ( ) No

4. Which of the following requirements do you currently have in place? *

- [x] Advanced Endpoint Protection (AEP)
- [x] Domain Migration Services (Migration to .gov)
- [x] Immutable Data Backup and Recovery Testing
- [ ] Multifactor Authentication Capability (MFA)
- [ ] All of the above
- [ ] None of the above

5. Project Name or Title *

Tillamook County Cybersecurity Assessment

6. Physical Address where the project will take place *

201 Laurel Ave., Tillamook, OR 97141

7. Amount of Funds Requested for this project. *

$24,700

8. Program or Project Point of Contact: Name *

Jeff Underwood

9. Program or Project Point of Contact: Title *

Information Technology Operations Manager

10. Program or Project Point of Contact: Phone Number *

(503)842-1800

11. Program or Project Point of Contact: Email Address *

jeff.underwood@tillamookcounty.gov

12. Program or Project Point of Contact: Mailing Address *

201 Laurel Ave.
Tillamook, OR, 97141

13. Fiscal or Accounting point of Contact: Name *

Shawn Blanchard

14. Fiscal or Accounting point of Contact: Title *

Treasurer

15. Fiscal or Accounting point of Contact: Phone Number *

(503)842-3439

16. Fiscal or Accounting point of Contact: Email Address *

shawn.blanchard@tillamookcounty.gov

17. Fiscal or Accounting point of Contact: Mailing Address *

201 Laurel Ave.
Tillamook, OR, 97141

18. SLCGP Service Catalog offering for this project *

- ◯ Advanced Endpoint Protection (AEP)
- ◯ Domain Migration Services (Migration to .gov)
- ◯ Immutable Data Backup and Recovery Testing
- ◯ Multifactor Authentication Capability (MFA)
- ◯ Albert Sensors
- ◯ Information Security Awareness Training
- ◯ URL/Web/Content filtering

- (●) Vulnerability Management Services & Scanning
- ( ) Consulting and Planning Services

19. Date your agency last completed the Nationwide Cybersecurity Review (NCSR) *

    In progress

20. Agency Federal Tax Identification Number *

    93-6002312

21. System for Award Management (SAM) Unique Entity Identifier Number: **UE-ID** *

    HEMCL199BU17

22. Remember to Right-Click and **Print** to "Save as a PDF" this page before you click the **Submit** button. You will need to save a copy for your records as well as upload it with your application in BaseCamp.

    Enter your answer

Fiscal Year 2022
State and Local Cybersecurity Grant Program
Project Application

Overview

This project application is for jurisdictions applying for the FY2022 State and Local Cybersecurity Grant Program (SLCGP). Every project submitted by a county, city, special district, or tribe must complete this application. No more than two project applications may be turned in per Applicant Agency.

I. General Project Information

Applicant Agency (agencies)
Tillamook County

Project Title
Tillamook County Cybersecurity Assessment

Federal Funds Requested
$24,700

SLCGP Service Catalog
Vulnerability Management Services Scanning

SLCGP Strategy **GOAL #**
3

SLCGP Strategy **OBJECTIVE #**
3.2

Project Budget Defined by POETE

Planning	$
Organization	$
Equipment	$
Training	$
Exercises	$24,700

POETE Areas	
Planning	Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
Organization	Individual teams, an overall organizational structure, and leadership at each level in the structure
Equipment	Equipment, supplies, and systems that comply with relevant standards
Training	Content and methods of delivery that comply with relevant training standards
Exercises	Exercises and actual incidents that provide an opportunity to demonstrate, evaluate, and improve the ability of core capabilities to perform assigned missions and tasks to standards

II. Requirements

Clearly describe how this project will address a cybersecurity gap/gaps, and how that will allow you to improve your current cyber capability.

Nexus of this project

The Nexus of this project lies in the comprehensive evaluation of the Counties cybersecurity. It involves a multi-faceted approach encompassing information gathering, understanding network and system architecture, and active and passive reconnaissance. The key objective is to identify vulnerabilities and potential attack vectors, without breaching the system, and thus, highlight potential risks for the organization. Risk assessment, documentation, and the delivery of a detailed report with recommended actions are pivotal components of this initiative. This project offers an opportunity for the organization to close existing cybersecurity gaps, enhance its current cyber capability, and fortify its security posture.

Cybersecurity Gaps

This project will identify any cybersecurity gap by examining the Counties cybersecurity network for potential vulnerabilities and weaknesses. Through a structured approach that includes information gathering, network architecture analysis, and various reconnaissance techniques, the project will uncover hidden security risks that might have otherwise gone unnoticed. Importantly, this assessment is conducted without actual system breaches, with a focus on illustrating potential risks. The subsequent risk assessment and documentation phase will offer a clear understanding of the severity and likelihood of exploitation for each identified vulnerability. This comprehensive approach enables the organization to prioritize and take immediate action to mitigate these vulnerabilities. The delivery of a detailed report with specific recommendations equips the organization with a roadmap to strengthen its cybersecurity defenses, effectively closing existing gaps and fortifying its overall security posture.

Current Cyber Capability Improvements

This project will significantly enhance our current cyber capability by providing a comprehensive and in-depth assessment of our system's vulnerabilities and potential attack vectors. With the systematic identification of weaknesses and potential risks, we will be better equipped to proactively address these issues before they can be exploited by malicious actors. The risk prioritization and actionable recommendations offered by the project will enable us to allocate our resources more effectively, focusing on the most critical vulnerabilities first and implementing measures to mitigate them. By doing so, we strengthen our overall security posture, reducing our exposure to cyber threats and fortifying our defenses.

The insights and best practices provided by this project will serve as a valuable knowledge base for our ongoing cybersecurity efforts. As we adopt industry

standards and security best practices, we can continuously improve our cyber capability, staying one step ahead of emerging threats. In essence, this project represents a pivotal step towards a more resilient and secure cyber environment, reducing the potential for data breaches, system disruptions, and reputational harm. It empowers us to actively manage our cybersecurity, ensuring that our organization is well-prepared to navigate the ever-evolving landscape of cyber threats.

Clearly describe how the project ties to Oregon's SLCGP Cybersecurity Plan.

Our project closely aligns with several key facets of the 2023 Oregon Cybersecurity Plan, demonstrating a proactive approach to addressing cybersecurity challenges and enhancing the state's overall cybersecurity resilience. Our project Aligns with the strategic goals and objectives set forth in the 2023 Oregon Cybersecurity Plan, providing a practical application of the state's cybersecurity framework. Here's an expanded overview of how your project aligns with the plan:

1. Comprehensive Information Gathering and Vulnerability Assessment (Strategic Goals 1 and 2):

Our project's initial phase, involving information gathering and vulnerability assessment, aligns closely with the strategic goals of cybersecurity governance and risk management outlined in the Oregon plan. Objective 1.2 of the plan emphasizes a risk-based approach to information security, and Our vulnerability analysis is designed to identify potential vulnerabilities and assess associated risks.

2. Vulnerability Analysis (Strategic Goals 2 and 5):

Our project's focus on vulnerability analysis and exploitation is in line with the objectives of measuring, assessing, and mitigating cyber risks and threats (Objective 2.2). We aim to categorize vulnerabilities based on severity and the likelihood of exploitation, which is consistent with the plan's emphasis on prioritizing remediation efforts based on risk.

3. Comprehensive Report and Recommendations (Strategic Goals 2 and 4):

Our projects commitment to providing a comprehensive report with recommendations for mitigation and best practices aligns with the objective of enhancing preparation, response, and resilience against cyber risk and threats (Objective 3.3). The plan also emphasizes building a culture of cyber awareness, and recommendations that can contribute to improving the organization's security posture.

4. Customized Approach (Strategic Goals 3, 4, and 6):

Our project's tailored and cost-effective approach aligns with the strategic goals of building a culture of cyber awareness and enhancing cybersecurity capabilities. It considers the organization's unique cybersecurity policies, supporting the objective of providing tailored security training and enhancing the security posture (Objective 7.1).

5. Flat-Rate Fee and Cost-Effective Measures (Strategic Goal 2):

The cost-effective approach aligns with the plan's objective of prioritizing risk-based cybersecurity investments (Objective 3.1). This ensures that the organization's resources are allocated efficiently to strengthen its cybersecurity.

III. Specific Requirements

Cyber Security

Has the jurisdiction performed a formal cyber assessment?
No

If the jurisdiction has not performed a formal cyber assessment, does the jurisdiction have a formal cyber security plan/strategy?
No

IV. Project Details 25pts

Describe the project. What will this project do? Please be as clear and direct as possible in your first paragraph. Supporting details may be provided in 2nd or 3rd paragraphs.

This project is strategically motivated by the necessity to proactively identify and address potential vulnerabilities within Tillamook Counties IT environment, aligning closely with the objectives outlined in the State of Oregon's 2023 Cybersecurity Plan (SLCGP). The primary business drivers include mitigating the risk of cyber threats, safeguarding sensitive information, ensuring data integrity, maintaining business continuity, and adhering to essential compliance requirements. The project's defined scope encompasses key activities such as information gathering, vulnerability analysis, and risk assessment, aiming to contribute significantly to the establishment of sound cybersecurity governance practices.

The total projected cost for the remote penetration test is $24,700, allocated to cover consultant fees for their specialized expertise, labor, and remote testing services. This investment is deemed essential as it addresses the critical need to fortify our cybersecurity defenses proactively. The consultant's comprehensive report, a crucial outcome of this investment, will not only highlight vulnerabilities but also provide actionable recommendations. This aligns seamlessly with the overarching goals of the SLCGP, contributing to improved risk management, mature cybersecurity capabilities, and the cultivation of a culture of cyber awareness within our organization.

In further detail, the budget breakdown encompasses various components, including consultant expertise, remote testing services, and comprehensive reporting. The consultant's role extends beyond the mere identification of vulnerabilities; it includes ensuring the effectiveness of our cybersecurity measures through quality assurance. This investment signifies a strategic commitment to

maintaining the integrity and confidentiality of our data, protecting our organizational reputation, and fortifying our systems against potential cyber threats. The expense of $24,700 is seen as justified given the potential consequences of a security breach and is integral to our overarching cybersecurity strategy.

Have you received quotes for the costs of the items, training, or services described above?

Yes

V. Project Impact 30pts

Describe who in the community will be directly impacted by this project and how.

The County Cybersecurity Assessment Project will significantly impact a diverse set of stakeholders within the community. County leadership and management will be directly influenced by the project's findings, shaping strategic decisions and resource allocations for bolstering cybersecurity measures. The internal IT and security teams will actively engage in the penetration test, implementing recommended improvements and enhancing their skills to mitigate cybersecurity risks. Additionally, employees, end users, customers, and clients will experience indirect benefits through a more secure digital environment, reducing the risk of data breaches and disruptions in services.

Regulatory authorities, compliance auditors, and business partners may also be affected, with the project potentially demonstrating compliance with regulations and fostering trust among business relationships. For more detailed information on the specific impacts on each stakeholder group, please refer to the attached Project Impact document

Describe what impact this project will have on the whole community.

The County Cybersecurity Assessment Project is a significant project with broad implications for the entire community. Its primary objective is to enhance cybersecurity measures within the County's systems, proactively safeguarding against evolving cyber threats. Given that the County IT and security teams manage crucial data and provide services vital to the entire population, the cyber assessment is a critical step toward mitigating the risk of major outages that could disrupt essential services. By gaining strategic insights from the project, county leadership can make informed resource allocations, strengthening the overall cybersecurity posture and contributing to a more secure digital environment that fosters trust and resilience in the face of potential threats.

The internal IT and security teams will play a central role in implementing the identified improvements, leading to enhanced data protection for employees, end users, customers, and clients. This initiative goes beyond organizational boundaries, positively impacting the wider community by reducing the risk of disruptions in County services. The overarching goal is to establish a robust and secure digital landscape that not only safeguards sensitive information but also aligns with industry cybersecurity standards, ensuring compliance and building a foundation of trust among stakeholders.

In addition to the immediate organizational impact, the County Cybersecurity Assessment Project holds significance for regulatory authorities, compliance auditors, and business partners. Potential improvements in regulatory compliance resulting from this initiative have the potential to strengthen trust in business relationships. The detailed insights provided in the attached Project Impact document underscore the County's commitment to creating a cyber-resilient community, cultivating a secure and compliant environment that benefits all stakeholders involved

Describe how the project will enhance the cyber capability for the jurisdiction.

The County Cybersecurity Enhancement Project is poised to significantly elevate the cyber capability of Tillamook County through a systematic approach. Conducting a thorough Vulnerability Assessment, the project will actively identify and address weaknesses in the County's IT infrastructure, offering a comprehensive understanding of its cybersecurity landscape. Subsequently, the initiative will focus on Risk Mitigation, calculating and documenting risks associated with identified vulnerabilities to prioritize and address them effectively. The project goes beyond technical aspects by providing actionable recommendations for improvement, fostering a cybersecurity culture within the County through increased awareness among employees and stakeholders. The detailed report, including proof of concepts for any exploited findings, serves as a roadmap for enhancing overall cybersecurity.

To measure the project's impact, key performance indicators and metrics have been established. Vulnerability Reduction will be assessed by tracking the decrease in high-risk vulnerabilities, while the Efficiency of Remediation will gauge the time taken for addressing and resolving identified issues. The project's success will also be evident in the realm of Improved Risk Management, contributing to a more accurate assessment of cybersecurity risks based on severity and likelihood. Ultimately, the Enhanced Security Posture of the County, as indicated by implemented recommendations and best practices, will serve as a pivotal indicator of the project's success. For more comprehensive details on the impact and evaluation methods, please refer to the attached Project Impact document.

VI. Capability History 5pts

Describe the jurisdiction's current functionality in the chosen cyber capability.

The County is actively enhancing its cybersecurity capabilities, acknowledging the need for substantial improvements in its current security posture. While efforts are underway to strengthen security measures, a comprehensive assessment is deemed necessary to identify vulnerabilities and determine the most effective next steps in fortifying the cybersecurity infrastructure. This evaluation will play a pivotal role in understanding the current functionality of the chosen cyber capability, guiding the development of a tailored strategy to bolster the organization's security posture proactively. By leveraging insights gained from the assessment, the county

aims to establish a robust and resilient cybersecurity framework, ensuring an effective defense against evolving cyber threats. For more detailed information on the county's cybersecurity history and capabilities, please refer to the attached Capability History document.
Currently, the county relies on a modest in-house cybersecurity team with varying levels of training and responsibilities. Recognizing the limitations of internal resources in addressing the evolving nature of cyber threats comprehensively, the county plans to augment its capabilities by introducing Managed Detection and Response (MDR) services. This strategic move aims to complement the existing team with external expertise in continuous monitoring, threat detection, and incident response. The collaboration with MDR services underscores the importance of combining internal knowledge with external support to enhance overall resilience and create a proactive cybersecurity posture against evolving threats. For a more in-depth understanding of the county's cybersecurity resources, skills, and capabilities, please refer to the attached Capability History document.

VII. Gap Information 15pts

Describe the current gap in the cyber capability.

Tillamook County is currently facing limitations in terms of time, equipment, and expertise to conduct a thorough assessment of our network vulnerabilities. The complexity of modern cybersecurity challenges demands a comprehensive evaluation, and our existing resources fall short in providing the in-depth analysis needed to identify and address potential threats effectively. Despite recognizing some low-hanging fruit, such as the implementation of multi-factor authentication, a more nuanced understanding of our network security needs is required to establish a robust and tailored strategy.

To bridge this gap, external assistance becomes crucial. Engaging with experts who possess the specialized knowledge and tools necessary for a detailed network assessment will enable us to gain insights into vulnerabilities that may have gone unnoticed. With this external support, we can develop a comprehensive plan for hardening our network, ensuring a proactive and resilient approach to cybersecurity.

Describe how the gap was identified (real event, exercise, assessment).

In 2020, the county experienced a significant setback when it fell victim to a cyberattack. In the aftermath of this incident, we recognized the pressing need to fortify our security infrastructure and protect sensitive data from future threats. In response, we initiated a series of measures to enhance our cybersecurity posture. However, acknowledging the evolving nature of cyber threats and the complexity of modern attacks, we have come to the realization that a comprehensive external assessment is essential to gain a thorough understanding of our current security position.

Since the cyberattack, we have been diligently working on internal improvements, implementing measures such as enhanced monitoring systems and employee training programs. These efforts represent our commitment to strengthening our defenses and mitigating potential vulnerabilities. To ensure that we have covered all bases and to identify any latent weaknesses, we have decided to seek the expertise of an external source. A comprehensive assessment from an outside perspective will provide us with a more objective and in-depth analysis, allowing us to make informed decisions on further security enhancements tailored to the specific challenges we face.

Describe what the agency/community has done to fill the gap so far.

To date, the county has taken proactive steps towards enhancing its cybersecurity resilience. Internal self-assessments have been conducted to identify and address potential vulnerabilities within our network infrastructure. Additionally, we have actively sought insights from other government organizations and engaged with vendors during conferences to gather valuable perspectives and ideas. These efforts have undoubtedly contributed to our progress in bolstering security measures, yet we recognize the need for a more extensive and specialized approach.

While self-assessments and collaboration with other entities have proven beneficial, the dynamic nature of cyber threats necessitates a comprehensive external review. We acknowledge that our current resources and experiences, though valuable, may have limitations in providing the depth of analysis required to navigate the intricacies of contemporary cybersecurity challenges. Therefore, we seek the assistance of professionals with extensive experience and knowledge in the field to thoroughly review our situation. This external perspective will offer a fresh and expert assessment, enabling us to identify blind spots, refine existing strategies, and implement measures that will have the greatest impact in fortifying our network security.

Recognizing the significance of cost-effectiveness, we are mindful of making prudent decisions that yield the most significant results with minimal expenditure. The expertise we seek will not only guide us in understanding our current security posture but will also provide recommendations for optimizing our cybersecurity strategy in a resource-efficient manner. This strategic approach ensures that our efforts are targeted and effective, aligning with our goal of fortifying the county's digital infrastructure against potential threats.

Describe how the proposed project will fill the gap.

The purposed assessment is a critical step in our ongoing commitment to fortify our cybersecurity defenses. By conducting a thorough examination of our current security landscape, we aim to pinpoint existing gaps and vulnerabilities within our network infrastructure. This insightful analysis will serve as the foundation for developing a comprehensive improvement plan tailored to our specific needs. Importantly, this is not a one-time initiative but marks the beginning of an ongoing process. Regular assessments are imperative to ensure that we are not only

making progress in addressing identified gaps but also to stay ahead of emerging threats.
The dynamic nature of cybersecurity demands a continuous and adaptive approach. Regular assessments will enable us to track our advancements, identify any new vulnerabilities that may arise, and adjust our strategies accordingly. By staying vigilant and regularly evaluating our security posture, we can proactively safeguard against potential risks, ensuring the resilience and efficacy of our cybersecurity measures in an ever-changing digital landscape.

VIII. Sustainment 15pts

Describe the jurisdiction's plan to sustain the cyber capabilities built by this project.
Tillamook County is actively constructing its cybersecurity infrastructure, with the proposed assessment serving as the foundational element for the development of a comprehensive Cybersecurity Plan. Although there is currently no pre-existing cybersecurity plan or documented strategy, the assessment results will offer crucial insights into vulnerabilities, risks, and areas requiring immediate attention. The county is committed to formulating a dynamic Cybersecurity Plan that will guide ongoing efforts, including strategic resource allocation, skill development, and continuous capability enhancement.
To sustain the cyber capabilities established by this project, the county will prioritize the identified needs based on assessment results. The plan encompasses funding provisions for ongoing investments in cybersecurity tools, technologies, and services, aligning with the strategic goals outlined in the cybersecurity plan. Skill development will be a priority, ensuring the cybersecurity team receives continuous training and education to stay ahead of evolving threats. The existing cybersecurity measures, such as Advanced Endpoint Protection, Domain Migration Services, and Immutable Data Backup and Recovery Testing, will be integrated into the broader cybersecurity plan, ensuring continuity and alignment with the overall strategy. For additional information, please refer to the attached Capability History document.

IX. Milestones 10pts

Quarter 1	Project Initiation
Quarter 2	Information Gathering Phase
Quarter 3	Vulnerability Analyses and Exploitation
Quarter 4	Risk Analysis and Documentation
Quarter 5	Report Generation

Quarter 6	Client Presentation and Review
Quarter 7	Project Closure and Documentation
Quarter 8	

Subapplicant: Tillamook County

Project Number: 1

Project Name: Tilllamook County Cybersecuity Assessment

Cyber Service	Consulting / Planning/Description of Expense	Total Cost	Agency	Discipline
Services & Scanning	Remote Penetration Test	$24,700	Tillamook County	General Government
		$0		
		$0		
		$0		
		$0		
		$0		
		$0		
		$0		
	Planning Subtotal	**$24,700**		

Cyber Service	Exercise / Training Course	Item/Expense	Number Trained	Total Cost	Agency	Discipline
				$0		
				$0		
				$0		
				$0		
				$0		
				$0		
				$0		
				$0		
	Training Subtotal			**$0**		

Cyber Service	Other /Description of Activities	Total Cost	Agency	Discipline
		$0		
		$0		
		$0		
		$0		
		$0		
		$0		
		$0		
		$0		
	Exercise Subtotal	**$0**		
	Equipment Subtotal	**$0**		
	PROJECT TOTAL	**$24,700**		

Tillamook County Cybersecurity Assessment

Project Impact

Introduction

Tillamook County was Established on December 15, 1853. The county is situated within Northwest Oregon along the coast, boasts a rich history and scenic beauty. With a current population of 27,390, the county encompasses communities such as Tillamook, Rockaway Beach, and Pacific City. Known for the Tillamook Cheese Factory, the county has historical ties to agriculture, timber, and fishing, with dairy farming being a significant economic contributor. Beyond its economic activities, Tillamook County's allure lies in its coastal landscapes, making it a hub for tourism and outdoor enthusiasts.

The Tillamook County Cybersecurity Assessment is a comprehensive project aimed at fortifying the digital resilience of our County. This multifaceted endeavor encompasses a systematic exploration of our IT landscape, employing a meticulous approach to gather information that forms the basis for understanding potential attack vectors and vulnerabilities. With approximately 300 users and 50 servers, this remote assessment follows a white box approach, utilizing credentialed scans where applicable, and includes a targeted review of operational and medical devices. The subsequent phases involve in-depth vulnerability analyses and exploitation, strategically aimed at identifying and mitigating potential risks without compromising system integrity. The project will conclude with the delivery of a detailed report, offering a comprehensive breakdown of identified vulnerabilities, actionable recommendations, best practices for heightened security, and proof of concepts for exploited findings. Through this project, we aspire not only to enhance our cybersecurity posture but also to foster a culture of awareness and resilience within our organization.

Direct Community Impact

The Tillamook County Cybersecurity Assessment is a critical project directly influencing numerous stakeholders within the community. These stakeholders, including County leadership, internal teams, employees, customers, regulatory authorities, and business partners, are integral to the organization or system undergoing examination. Given the County's role in managing data and delivering services to the entire community, cyber assessment becomes a crucial tool for enhancing data protection. The project aims to minimize the risk of significant outages that could impede service delivery by identifying vulnerabilities and promptly addressing them. This initiative ensures the uninterrupted provision of essential services, directly benefiting the broader community.

Key Individuals and Groups Affected:

The project's impact extends to key individuals and groups within the community. County leadership and management teams are directly influenced as penetration test findings guide strategic decisions, resource allocations, and cybersecurity enhancements. Internal IT and security teams actively participate in the assessment, implementing recommended improvements and enhancing their skills to mitigate risks. While all employees and end users indirectly benefit from a more secure digital environment, customers and clients relying on County services experience improved data protection and security. Business partners and suppliers are reassured by a successful penetration test, fostering trust in the security of their data and interactions with the County.

Impact on County Services:

The cybersecurity enhancement initiative directly addresses various county services, impacting functions such as clerks recording deeds, tax assessment and collection, community development planning, and emergency

management. The attack carried out on February 3, 2020, by the REvil cybercriminal organization further underscores the vulnerability of county systems. Despite efforts to avoid ransom payment, the incident resulted in a significant financial loss of $300,000 emphasizing the importance of robust cybersecurity measures. The forensic investigation concluded with no evidence of personal information access or theft from employees or residents. The incident's impact on the community, including server downtime, disruptions to internal systems, and the disabling of network connections to contain malware spread, highlights the urgency of addressing cybersecurity challenges in the digital age.

Please refer to the examples provided below for a more detailed breakdown of how the outcomes of this project will affect the county service crucial to the community:

Clerk's office: **potential disruption in recording deeds and documents:** The County Cybersecurity Assessment ensures the cybersecurity of systems critical to clerks' operations. This helps safeguard against potential disruptions, ensuring the smooth recording of deeds and documents without the risk of cybersecurity incidents affecting data integrity.

Tax office: Risk to assessment, tax levy, and collection processes: Risk to assessment, tax levy, and collection processes: The project mitigates risks associated with the assessment, tax levy, and collection processes. By identifying vulnerabilities, it prevents potential cyber threats that could disrupt or compromise these crucial financial operations.

Community Development: Impact on planning and sanitation services: The project's enhancements secure systems vital to community development operations. This ensures uninterrupted planning and sanitation services, safeguarding against potential cyber disruptions that could impact community development initiatives.

Emergency Management: Redirected resources and loss of network during incidents: The assessment contributes to emergency management by preventing potential cyber incidents that could redirect resources. It ensures the network remains intact during critical incidents, allowing for effective communication and resource allocation.

Health Services: Disruption in public health services such as restaurant inspections and immunizations: With a focus on cybersecurity, the project safeguards public health services. This prevents disruptions, such as delays in restaurant inspections and immunizations, ensuring the community's health and well-being are not compromised by cyber incidents.

Sheriff's Office: Challenges across all law enforcement factors, including patrol and jail operations: The project addresses vulnerabilities within law enforcement systems, minimizing the potential for disruptions in various operational aspects, such as patrol and jail operations.

County Treasurer: Potential delays in issuing paychecks and processing invoice payments: Cybersecurity enhancements from the project secure financial systems. This prevents potential delays in issuing paychecks and processing invoice payments, ensuring the treasurer's operations remain efficient and free from cyber-related disruptions.

Whole Community Impact

The impact of the penetration test project on the community is evident in its direct benefits to cybersecurity, data protection, and service continuity. Firstly, the project significantly enhances the community's cybersecurity posture by fortifying the security of the organization's systems. This not only protects the organization but also safeguards the data and digital interactions of every community member. The tangible reduction in the risk of cyberattacks and data breaches fosters a safer digital environment, ensuring the well-being of all individuals connected to the community.

Secondly, the project positively influences data protection and privacy for everyone in the community whose data is managed by the County. Strengthened security measures contribute to maintaining privacy and trust in digital interactions. Addressing vulnerabilities ensures that sensitive information remains confidential and secure, building a foundation of digital trust within the community.

Lastly, the community benefits from the project's emphasis on ensuring the continuity of services. Clients and customers reliant on the County's services can access them without disruptions caused by potential cyber incidents. This reliability contributes to the overall stability of the community, ensuring essential services remain available, allowing community members to engage in their digital activities with confidence and convenience.

Impact on County Services and Cyberattack Incident:

The major impacts on county services are notable across various functions such as clerks recording deeds, tax assessment and collection, community development planning, emergency management, public health services, law enforcement, and financial operations. The cyberattack, reportedly orchestrated by the international cybercriminal organization REvil, disabled the county's computer system for around two weeks. Despite the county's efforts to avoid ransom payment through backup solutions, data critical to county operations could only be restored by paying the cyber attacker for decryption keys. The $300,000 financial loss has significant implications for the rural county's finances, with additional costs yet to be determined. The incident underscores the evolving security hazards in the digital age, prompting the need for prompt disclosure and heightened cybersecurity measures. County systems are now operational following security measures, and a concluded forensic investigation found no evidence of personal information access or theft. The cyberattack origin from the REvil group, known for its lucrative "ransomware-as-a-service" operation, emphasizes the importance of disclosing incidents promptly to alert business partners and customers.

Enhancement of Cyber capability of the County

The penetration test project serves as a cornerstone in enhancing the cyber capability of the County, systematically addressing vulnerabilities, and fortifying its overall cybersecurity posture. The key components of this enhancement strategy include:

1. **Vulnerability Assessment:** The project initiates a comprehensive vulnerability assessment, actively and passively gathering information about the County's IT systems. This identifies vulnerabilities, weaknesses, and potential security risks, establishing a clear understanding of the cybersecurity landscape.
2. **Risk Mitigation:** Following vulnerability identification, the project calculates and documents risks based on discovered vulnerabilities. Rather than attempting to breach the system, this risk assessment prioritizes and addresses vulnerabilities effectively, aiming to assess the severity and likelihood of potential threats.
3. **Actionable Recommendations:** The project provides a detailed report outlining identified vulnerabilities, actionable recommendations for mitigation, and best practices for enhancing overall cybersecurity. Proof of concepts for any exploited findings further contributes to the practical implementation of cybersecurity measures.
4. **Cybersecurity Culture:** Beyond technical aspects, the project fosters a cybersecurity culture within the County. Through heightened awareness during the testing process, employees and stakeholders become more vigilant and proactive in identifying and responding to security threats.

Measurement of Cyber Capability Enhancement:

Measuring the success of the cyber capability enhancement involves key performance indicators and metrics focusing on reduction, efficiency, and improvement:

1. **Vulnerability Reduction:** Success is gauged by the reduction in the number of identified vulnerabilities, particularly those posing high risks to the County's cybersecurity.
2. **Efficiency of Remediation:** The time taken to address and remediate vulnerabilities is assessed, with a successful outcome involving faster resolution times.
3. **Improved Risk Management:** The project contributes to a more accurate assessment of risk, considering vulnerability severity and threat likelihood. This aids the County in prioritizing and managing cybersecurity risks more effectively.
4. **Enhanced Security Posture:** Overall improvement in the County's security posture, as evidenced by the implementation of recommendations and best practices, serves as a key indicator of success.

Impact on County Services and Cyberattack Incident:

This cyber capability enhancement is particularly crucial considering a recent cyberattack reportedly orchestrated by the international cybercriminal organization REvil. The attack disabled the County's computer system for two weeks, emphasizing the importance of implementing new security measures. Despite exhaustive efforts to avoid ransom payment, the $300,000 loss has significant financial implications for the rural county. The cyberattack highlights the emerging security hazards in the digital age. The conclusion of a forensic investigation found no evidence of personal information access or theft, affirming the government's victimhood in this crime. The incident underscores the imperative for prompt disclosure and heightened cybersecurity measures. The County's systems are now operational, emphasizing the need for ongoing vigilance and preparedness to prevent and respond to future cyber threats.

In summary, the penetration test project significantly enhances the County's cyber capability by systematically addressing vulnerabilities, assessing risks, and providing actionable recommendations. This holistic approach not only strengthens the technical aspects of cybersecurity but also instills a culture of heightened awareness and proactive security measures. Success will be reflected in reduced vulnerabilities, efficient risk management, and an overall bolstered cybersecurity posture.

Tillamook County Cybersecurity Assessment Milestones

The milestone list is a high-level view of the project for planning purposes. Each milestone has a duration, and the overall project timeline is given. Please note that most tasks occur in parallel to achieve the overall timeline milestone goal. Many of the tasks performed during detailed planning have either been completed or are substantially complete so the total project time is extremely compressed.

Presented below is a comprehensive roadmap outlining key milestones for the Tillamook County Cybersecurity Assessment —a remote penetration test. This initiative is designed to enhance cybersecurity resilience by identifying and mitigating potential vulnerabilities in our digital infrastructure. The milestones outlined below have been strategically crafted to ensure the success of the penetration test, reflecting our commitment to bolstering the security posture of our organization. We believe that achieving these milestones will significantly contribute to safeguarding our digital assets and, by extension, the sensitive information of our stakeholders.

Milestone 1: Project Initiation (April 1, 2024 - May 31, 2024)

- Conduct initial project kickoff meeting.
- Define project scope, objectives, and deliverables.
- Assemble project team and allocate responsibilities.
- Establish communication and reporting protocols.

Milestone 2: Information Gathering Phase (June 1, 2024 - September 30, 2024)

- Collect publicly available information about the organization.
- Develop a detailed understanding of the target's network and system architecture.
- Conduct passive reconnaissance techniques.
- Document the organization's IT environment and security considerations.

Milestone 3: Vulnerability Analyses and Exploitation (October 1, 2024 - January 31, 2025)

- Identify potential vulnerabilities within the target system.
- Perform active, manual attempts to utilize exploits (with agreed and permitted access).
- Calculate and document risks based on discovered vulnerabilities.
- Develop a scoring system for severity and likelihood of threats.

Milestone 4: Risk Analysis and Documentation (February 1, 2025 - May 31, 2025)

- Analyze risks associated with identified vulnerabilities.
- Score vulnerabilities based on severity and likelihood of a threat.
- Document all findings for inclusion in the final report.
- Conduct an internal review of documented vulnerabilities and risks.

Milestone 5: Report Generation (June 1, 2025 - September 30, 2025)

- Compile a comprehensive report detailing identified vulnerabilities.

- Provide recommendations for mitigating identified vulnerabilities.
- Outline best practices to enhance overall security posture.
- Develop proof of concepts for exploited findings.

Milestone 6: Client Presentation and Review (October 1, 2025 - November 30, 2025)

- Schedule and conduct a presentation for the client.
- Review assessment findings, recommendations, and best practices.
- Address any questions or concerns raised by the client.
- Collect feedback for final adjustments to the report.

Milestone 7: Project Closure and Documentation (December 1, 2025 - March 31, 2026)

- Finalize the comprehensive assessment report.
- Ensure all client feedback is incorporated.
- Complete any remaining documentation or administrative tasks.
- Officially close the project and archive project materials.

In conclusion, the Tillamook County Cybersecurity Assessment's meticulously outlined milestones signify our unwavering dedication to fortifying our digital defenses. As we begin this remote penetration test, each phase from project initiation to closure has been thoughtfully designed to maximize the effectiveness of our cybersecurity measures. The comprehensive report generated at the project's culmination will not only detail identified vulnerabilities but also provide actionable recommendations and proof of concepts, ensuring a robust security posture for our organization. We believe that these strategic milestones, coupled with your support, will play a pivotal role in safeguarding our digital assets and maintaining the trust of our valued stakeholders.

Tillamook County Cybersecurity Assessment Capability History

County's current functionality in the chosen cybersecurity capability

The county is currently in the process of enhancing its cybersecurity capabilities, recognizing a need for significant improvement in its current security posture. The existing functionality reveals vulnerabilities that need careful examination to better understand and address potential weaknesses. While efforts are underway to strengthen security measures, a comprehensive assessment is deemed necessary to ascertain the specific areas where the organization is relatively weak and to determine the most effective next steps in fortifying our cybersecurity infrastructure.

The assessment will play a pivotal role in evaluating the jurisdiction's current functionality in the chosen cyber capability. This examination will provide a detailed and nuanced understanding of the existing security landscape, helping to identify gaps and areas requiring immediate attention. The insights gained from the assessment will guide the development of a tailored strategy, outlining the best course of action to bolster the organization's overall security posture. By undergoing this thorough evaluation, the county aims to lay the groundwork for a robust and resilient cybersecurity framework, ensuring a proactive and effective defense against evolving cyber threats.

County's Current Cybersecurity Resources

Currently, the county relies on a modest in-house cybersecurity team, comprising three staff members with varying levels of training and responsibilities in cybersecurity. While none of these individuals have cybersecurity as their primary job function, the responsibilities are distributed among the Systems Administrator, Network and Operations Tech, and Operations Manager. Despite their diverse roles, these team members share the collective responsibility of managing and mitigating cybersecurity risks within the organization. As the digital landscape becomes increasingly complex, there is a recognition that the existing internal resources may be limited in addressing the evolving nature of cyber threats comprehensively.

To augment and strengthen the county's cybersecurity capabilities, there is an intention to bring in Managed Detection and Response (MDR) services. This strategic move aims to complement the existing internal resources by leveraging external expertise in continuous monitoring, threat detection, and incident response. By adding MDR to the cybersecurity strategy, the county seeks to enhance its overall resilience, leveraging specialized skills and tools to fortify defenses and respond effectively to potential security incidents. This collaborative approach acknowledges the importance of combining internal knowledge with external support to create a more robust and proactive cybersecurity posture in the face of ever-evolving cyber threats.

County's Current Cybersecurity Skills

The county's current cybersecurity team is equipped with a solid foundation of skills, featuring a CISSP (Certified Information Systems Security Professional) certified staff member and a Security+ certified staff member. The CISSP certification signifies a high level of expertise in designing, implementing, and managing security programs, while the Security+ certification demonstrates proficiency in foundational cybersecurity skills and knowledge. With these certified professionals, the county demonstrates a commitment to maintaining a skilled workforce capable of navigating the complex landscape of cybersecurity challenges. These certifications underscore the importance placed on adhering to industry best practices and standards, positioning the county to address and mitigate potential security risks effectively.

County's Current Cybersecurity Capabilities

The county has been actively enhancing its cybersecurity capabilities with a series of strategic measures. Currently in progress is the implementation of Multi-Factor Authentication (MFA) for email, utilizing YubiKey, with plans to extend this security measure to VPN access for all staff. This approach not only adds an additional layer of protection to email communications but also reinforces secure remote access. Importantly, the use of YubiKey for administrative access to servers further heightens security measures, aligning with best practices in access control and authentication.

To fortify endpoint protection, the county has deployed Sophos Intercept x + XDR, offering advanced threat detection and response capabilities. The implementation of a web application firewall for external-facing web servers adds an additional layer of defense against potential cyber threats. The utilization of Splunk for log collection enhances the county's ability to monitor and respond to security incidents, with specific notifications in place for locked network accounts and off-hours administrative logins. In a proactive stance against ransomware, the county has implemented cloud immutable backups, providing an extra layer of resilience by ensuring data recoverability in the event of a security incident. These comprehensive cybersecurity measures collectively contribute to the county's efforts to establish a robust and resilient defense against a wide range of cyber threats.

APPENDIX B

PLEASE COMPLETE ALL SECTIONS IN YELLOW. WHERE DOLLAR AMOUNT DOES NOT APPLY LEAVE AT $0.00
THIS FORM IS FILLABLE. AMOUNTS & TOTALS WILL CALCULATE AUTOMATICALLY

TILLAMOOK COUNTY TRAVEL AUTHORIZATION 01/01/2024-12/31/2024

Please complete this form and obtain required signatures *before* traveling.

1. *Name of Employee/Traveler:* ERIN SKAAR
2. *Date:* 12/22/2023
3. *Training Related/Conference (if yes, attach Agenda):* ○ Yes ◉ No
4. *Airfare/Railfare:* $ 527.00 Confirmation Number:
5. *Name of Conference or Training:* National Association of Counties (NACo) Legislative Conference
6. *Conference/Training Cost:* $ 575.00
7. *Itinerary:*
   Destination (City, State): Washington, DC
   Est. Departure Date: 2/9/2024 Time: 6:00 am
   Est. Return Date: 2/14/2024 Time: 9:30pm
8. *Lodging Reservation Information:*
   Hotel Name: WASHINGTON HILTON
   Address: 1919 CONNETICUT AVE NW
   WASHINGTON, DC 20009
   Phone number: 888-751-5182
   Confirmation Number:
9. *Miscellaneous Expenses:*
   (Identify Specific Expenses: Taxis, Shuttles, Etc.)
   a. Airport transportation/shuttles $ 100.00
   b. PDX Airport Parking fees $ 125.00
   c.
   d.
10. *Lodging Rate:*

Amount per Night:	$ 275.00
Tax per Night:	$ 41.11
Total per Night:	$ 316.11
Number of Nights: x	5
Total Lodging:	$ 1,580.55

11. *Meals:* **(Please CHECK which rate you are using in ONE box below)**
    Daily Meal Rate without receipts (See policy): ☐
    CONUS Rate with detailed receipts and accounting: ☐
    *Daily Rate: $ 59.00 *(Standard rate or City Conus Rate)

	# of Meals	x Rate	Total
Breakfast:	5	$ 11.80	$ 59.00
Lunch:	3	$ 17.70	$ 53.10
Dinner:	5	$ 29.50	$ 147.50
		Total Meals:	$ $ 259.60

12. *Cost of Trip:*

Airfare/Railfare:	$ 527.00
Lodging:	$ 1,580.55
Meal Per Diem:	$ 259.60
Personal Car Miles:	$ 113.63
Training/Conference Cost:	$ 575.00
Miscellaneous:	$ 225.00
Total Not To Exceed:	$ 3,280.78

13. *Personal Car Miles*

		IRS Rate	Total
Total miles round trip:	169.6 x	0.67 $	$ 113.63

14. *Purpose of Trip (Be Specific):*
    Attending the National Association of Counties (NACo) Legislative Conference in Washington DC

    ESTIMATED TRAVEL DATES & EXPENSES. HOTEL BASED ON AVAILABILITY AND SUBJECT TO CHANGE.

15. *Approved for Payment:*

Meal Per Diem:	$ 259.60	Transportation:	$ 527.00
Personal Car Miles:	$ 113.63	Training/Conference:	$ 575.00
Misc:	$ 225.00	Total	$ 3,280.78
Lodging:	$ 1,580.55		

16. *Employee/Traveler Signature:* Erin Skaar — *Date:* 1/3/2024
17. *Department Head/Designee Signature:* Rachel Hayes — *Date:* 12/29/2023
18. *Board of Commissioner's Signature (Required for Out-Of-State)* MF BM — *Date:* 1/3/2024

Rev. 12/14/23

APPENDIX D

TILLAMOOK COUNTY

REQUEST APPROVAL FORM TO UTILIZE EMPLOYEE/AGENT PRIVATE VEHICLE FOR COUNTY BUSINESS

APPROVAL REQUIRED PRIOR TO USAGE OF PRIVATE VEHICLE

Destinations:

TO: Portland_____FROM: Tillamook_____

I request approval to use my private vehicle on 2/9/2024-2/14/2024 for Tillamook County business purpose of:
Attending NACO conference in Washington DC.

Reason for using private vs. County owned vehicle is:
Personal use of vehicle during trip

I am (x) am not ( ) requesting mileage reimbursement. Insurance terms remain the same whether or not mileage payment is requested. This form must accompany the reimbursement request.

Personal or Private Vehicle Liability. If you authorize your employees/agents to use a personal or private vehicle on County business, he/she is responsible to carry the minimum liability insurance required by law (must provide proof before department head/designee approval). If employees operate a personal or private vehicle on County business, their personal liability insurance policy is primary and County coverage is excess. If the amount of liability to third parties exceeds their private policy limits, the County will provide excess liability coverage.

The County does not cover collision or comprehensive insurance for personal vehicles. When utilizing a personal vehicle for County purposes, the employee/agent is 100% responsible for collision or comprehensive damage incurred to the vehicle.

The rationale of having County employees/agents complete a vehicle usage form is for their own knowledge pertaining to County vehicle coverage, and liability protection from the County. Plus, the signed form may give their department head/designee a heads up as to who will be using their own vehicle on County business and committing department funds when claiming reimbursement for personal vehicle mileage. The signing of the personal vehicle usage document will inform the County employee/agent that their insurance is the first to be used in the event of a vehicle accident. Each department should keep a copy of the signed form on file.

If involved in an accident while on official County business, I will advise the Human Resources Department within twenty-four (24) hours by calling 503-842-3418.

Employee: MF Bled Date: 01 03 24

Department Head/Designee Rebecca Hayes Date: 12/29/2023

STATEMENT OF MILEAGE AND EXPENSE / TRAVEL EXPENSE DETAIL

CLAIMANT NAME: ERIN SKAAR **MONTH OF:** Feb-24

2024 MILEAGE RATE: $.67 *Mileage rate is subject to IRS updates.
***01/01/2024-12/31/2024**

DATE	DESCRIPTION	MILES		EXPENSE AMOUNT
2/9--2/14/2024	Mileage to Portland airport return trip			
	84.8 miles each way from Tillamook	169.60		
2/9--2/14/2024	Per Diem			259.60
2/9--2/14/2024	Airport Parking & shuttles			225.00
	PER DIEM, PARKING & SHUTTLE EXPENSES			
	ARE ESTIMATED AND SUBJECT TO CHANGE			
	TOTAL EXPENSES			$ 484.60
	TOTAL MILEAGE	169.60	0.67	$ 113.63
	TOTAL THIS REIMBURSEMENT REQUEST			$ 598.23

Approved for Payment

I certify that the above claimed expenses are authorized duty required expenses. Funds for payment of this claim are available in the approved budget for the period covered and have been allotted for expenditure.

Richard Hayes 12/29/2023

Authorized Signature

I certify that the within bill for services rendered and expenses incurred was to furnished Tillamook County, Oregon. That the items shown therein were not for the use or benefit of any individual person, but solely for the use and benefit of Tillamook County. That the prices charged therein are reasonable, and that the same is wholly unpaid.

MF Bell 01 03 24

Claimant Signature

ESTIMATED - NACO LEGISLATIVE CONFERENCE PER DIEM – ERIN SKAAR

FRIDAY – 2/9/24	Breakfast	Lunch	Dinner
SATURDAY – 2/10/24	Breakfast		Dinner
SUNDAY – 2/11/24	Breakfast		Dinner
MONDAY – 2/12/24	Breakfast	Lunch	Dinner
TUESDAY – 2/13/24	Breakfast	Lunch	Dinner

/ EVENTS

2024 NACo Legislative Conference

JUMP TO SECTION:

About the Conference

The National Association of Counties (NACo) Legislative Conference brings together nearly 2,000 elected and appointed county officials to focus on federal policy issues that impact counties and our residents.

Attendees have the opportunity to engage in second-to-none policy sessions, meet the members of the 118th Congress and interact with federal agency officials.

This is a one-of-a-kind advocacy opportunity to strengthen our intergovernmental partnerships for years to come.

Register Today

Access our registration portal here to register for the conference.

For questions or assistance with registration contact us via email or phone at 202.942.4292 or nacomeetings@naco.org and indicate "Leg Conference 2024" in the subject line.

Register Today

Registration Rates

	ADVANCED	ON-SITE
	Rates valid Dec. 9, 2023 – Jan. 26, 2024	*After Jan. 27*
NACo Member County	$575	$690
Non-Member County	$810	$960
NACo Corporate Member	$650	$780
Corporate Non-Member	$890	$1060
Government *Federal or state employees only*	$650	$780
CIO-Forum *Pre-conference event*	$100	$100

Registration Policies

For questions with registration, view the details below or contact us via email or phone at 202.942.4292 or nacomeetings@naco.org.

Press Registration

Members of the press are invited to request consideration for press credentials.

To do so, please complete the **contact form at the bottom of the page** and select "Media Inquiries & Press Registration" as the message type.

Guest Registration

Partner/Spouse

- **Registrations include:** the conference-wide Football Watch Party reception event and general sessions. For travel companions only. Not valid for colleagues and those with related job functions.
- **Registration Rate:** $60

Guest Age 6 to 18

- **Registration includes:** the conference-wide Football Watch Party reception event and general sessions. For travel companions only.
- **Registration Rate:** $30

Guest Age 5 & Under

- **Registration includes:** the conference-wide Football Watch Party reception event. For travel companions only.
- **Registration Rate:** Free

Payment Policy

Payment is due at the time of registration. Exceptions can be made to allow for payment by check on a case by case basis. All fees must be paid in full prior to arrival in order to obtain your badge and registration materials at the conference.

Contact nacomeetings@naco.org with any questions.

Cancellation Policy

Registrations cancelled by January 5, 2024 will be refunded less a $50 administration fee. Cancellation requests made between January 6 and January 31 will receive a 50 percent refund. (This applies to all registration types including guest and spouse fees.) Refunds will not be available after January 31, 2024, including for unused registrations or "no-shows."

All cancellations must be made in writing by emailing cancellations@naco.org.

Registration Transfers & Substitutions

To transfer a registration, please contact nacomeetings@naco.org and provide the name and email of the person whose registration you are transferring and the name and email address of the person to whom the registration should be reassigned.

FIND LOCAL SOLUTIONS

Federal Agency Expo

Tuesday, February 13 | 9:00 a.m. - 11:30 a.m. EST

NACo's Federal Agency Expo convenes over 100 federal officials representing dozens of offices in one place, ready to engage with conference attendees.

LEARN MORE ABOUT LAST YEAR'S PARTICIPANTS

Conference Schedule

All times listed in Eastern Standard Time.

For purposes of travel planning, check out the schedule at a glance.

Stay tuned for the full schedule of events and workshops coming soon!

Friday, Feb. 9

Pre-Conference

8:00 a.m. – 5:00 p.m.	FEMA Just-in-Time Recovery Management Training This session is limited to the first 75 attendees to RSVP through the conference registration process. There is no cost to participate, but please only register if you plan to attend so we can host as many attendees as possible.
9:00 a.m. – 10:00 a.m.	CIO Technology Speed Sharing
10:30 a.m. – 5:00 p.m.	CIO Forum
5:30 p.m. – 7:00 p.m.	CIO Forum Reception

Saturday, Feb. 10

8:00 a.m. – 9:30 a.m.	First-Time Attendee Orientation (Open to first-time attendees only)
9:30 a.m. – 4:30 p.m.	Policy Steering Committee Meetings ■ Agriculture and Rural Affairs ■ Health ■ Public Lands ■ Human Services and Education ■ Finance, Pensions and Intergovernmental Affairs ■ Transportation ■ Community, Economic and Workforce Development ■ Telecommunications and Technology ■ Environment, Energy and Land Use ■ Justice and Public Safety
5:00 p.m. – 8:00 p.m.	Affiliate & State Association Meetings/Receptions

Sunday, Feb. 11

7:00 a.m. – 7:45 a.m.	Non-Denominational Worship Service
8:00 a.m. – 9:45 a.m.	GIS Subcommittee Meeting
8:00 a.m. – 9:45 a.m.	Immigration Reform Task Force (IRTF) Meeting
8:00 a.m. – 9:45 a.m.	Arts & Culture Commission Meeting
8:00 a.m. – 9:45 a.m.	Resilient Counties Advisory Board Breakfast

9:00 a.m. – 11:00 a.m.	Large Urban County Caucus (LUCC) Meeting
10:00 a.m. – 12:00 p.m.	Rural Action Caucus (RAC) Meeting
10:00 a.m. – 12:00 p.m.	IT Standing Committee Meeting
12:00 p.m. – 1:30 p.m.	Membership Standing Committee Meeting
12:00 p.m. – 1:30 p.m.	Healthy Counties Advisory Board Lunch
2:00 p.m. – 4:00 p.m.	Western Interstate Region (WIR) Meeting
2:00 p.m. – 4:00 p.m.	Veterans and Military Services Committee Meeting
2:00 p.m. – 4:00 p.m.	International Economic Development (IED) Task Force Meeting
2:00 p.m. – 3:00 p.m.	Programs and Services Committee Meeting
2:00 p.m. – 4:00 p.m.	Gulf States, Counties and Parishes Caucus Meeting
2:00 p.m. – 4:45 p.m.	Workshops, topics including: ■ Immigration law ■ Earmarks and grants ■ Transportation ■ Waters of the U.S. (WOTUS) ■ Infrastructure ■ Intergovernmental partnership

3:15 p.m. – 4:45 p.m.	Board of Directors Forum
6:00 p.m. – 10:00 p.m.	Football Watch Party

Monday, Feb. 12

8:00 a.m. – 9:00 a.m.	Central Region Caucus Meeting
8:00 a.m. – 9:00 a.m.	Northeast Region Caucus Meeting
8:00 a.m. – 9:00 a.m.	South Region Caucus Meeting
8:00 a.m. – 9:00 a.m.	West Region Caucus Meeting
9:30 a.m. – 11:30 a.m.	General Session
11:45 a.m. – 1:30 p.m.	Affiliate & State Association Lunches
12:30 p.m. – 2:30 p.m.	Board of Directors Meeting
1:30 p.m. – 2:45 p.m.	Workshops, topics including: ■ Policy priorities ■ Solutions for counties from NACo EDGE

3:30 p.m. – 5:00 p.m.	Policy Summits: ■ Counties Ready for 2024: NACo Summit on Election Administration ■ Disasters & Resiliency: NACo Summit on County Finances and Property Insurance ■ County Artificial Intelligence Summit hosted by the NACo AI Exploratory Committee
5:00 p.m. – 7:00 p.m.	State Association and Affiliate Meetings and Receptions
6:30 p.m. – 9:00 p.m.	LUCC/RAC/Board of Directors Dinner Reception Open to members of LUCC, RAC and the Board of Directors

Tuesday, Feb. 13

8:00 a.m. – 9:30 a.m.	Military Communities Network Breakfast
9:00 a.m. – 11:30 a.m.	Federal Agency Expo & Breakfast *Learn more about last year's federal agency participants **here**.*
11:30 a.m. – 11:45 a.m.	All-Conference Photo
12:00 p.m. – 5:00 p.m.	Capitol Hill Day of Action
12:00 p.m. – 5:00 p.m.	Open House at NACo HQ

4:30 p.m. – 6:30 p.m.	Closing Reception on Capitol Hill

Housing

Nestled in between the urban Adams Morgan & Dupont Circle neighborhoods, The Washington Hilton will host all conference sessions unless otherwise noted in the program. Special rates have been secured at both the Hilton and the Churchill Hotel, but you must register for the conference before booking your room. All conference sessions will be held at the Washington Hilton unless otherwise noted in the program. Inventory at the Hilton is extremely limited and may indicate sold out status for your dates; we recommend booking a room at one of the overflow rooms if you cannot book at the Hilton.

Washington Hilton

1919 Connecticut Avenue NW Washington, DC 20009

Room Rate: $275 single/double occupancy

The Churchill

1914 Connecticut Avenue, NW Washington, DC 20009

Room Rate: $265 single/double occupancy

Hotel Rates & Cancellation

All rates are quoted exclusive of applicable D.C. taxes (currently at 14.95%). Room block rates are good through January 12, 2024 and available on a first-come, first-serve basis. Note: Rooms may sell out early; once the block is sold out, the hotel's market price applies regardless of the date of booking. Please confirm all cancelation policies and deposit requirements when booking your reservation.

At the Hilton, cancelations made within 72 hours of arrival will be charged for one night's room and tax; at the Churchill, cancelations made within 48 hours of arrival will be charged for one night's room and tax. Any cancellation charges incurred are the responsibility of the attendee. Please contact your selected hotel directly if you need to make changes or cancel your reservation.

Health & Safety

NACo is offering in-person attendance at its 2024 NACo Legislative Conference pursuant to local government orders and public health guidance on such gatherings. NACo is committed to hosting a safe event for all participants and to this end requires all members, guests, staff and supplier personnel to comply with safety precautions specified for Washington, D.C. and the Washington Hilton Hotel in addition to state, local government and CDC guidelines and recommendations.

Learn More: 2024 Legislative Conference **Waiver of Liability** and **Code of Conduct**.

Contact Us

Have a question? NACo is here to help!

Please complete the contact form and NACo staff will reach out to provide assistance. Alternatively, email nacomeetings@naco.org or call 202.942.4292.

Name *

First | Last

Title * | **Email ***

Organization * | **State ***

State

Message Type *

No change fees for all flights
You can change these flights without paying a fee if plans change. Because flexibility matters.

Portland to Washington

9:37am - 5:30pm (4h 53m, nonstop)
Alaska Airlines • Fri, Feb 9

Average CO_2

Show details

Your fare: Main

Upgrade for $100 roundtrip to get a refundable fare.

See upgrade options

Washington to Portland

6:30pm - 9:28pm (5h 58m, nonstop)
Alaska Airlines • Wed, Feb 14

Above average CO_2

Show details

Your fare: Main

Upgrade for $100 roundtrip to get a refundable fare.

See upgrade options

Seats

Seat choice included

Choo

Trip total
$527
View price summary

Check out

Bags

✓ Carry-on bag included

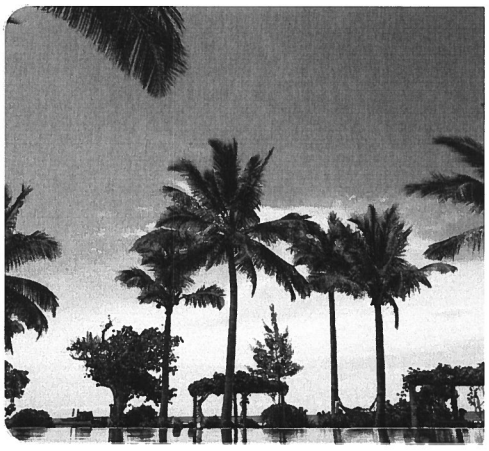
$ 1st checked bag for a fee

Bags for this flight must be purchased through the airline after booking.

Free cancellation
There's no fee to cancel within 24 hours of booking.

Tell us how we can improve our site

Share feedback



Go further with the Expedia app

Save even more - get up to 20% on select hotels when you book on the app. Our app deals help you to save on trips so you can travel more and manage it all on the go.

Switch to the app

expedia group

Company

About

Jobs

Trip total
$527

PARKING AT PDX

For Assistance: Call 503.460.4234 - Available daily from 7:30 a.m. - 9 p.m.

Payment Methods: PDX accepts cash, debit cards, American Express, Discover, MasterCard and Visa.

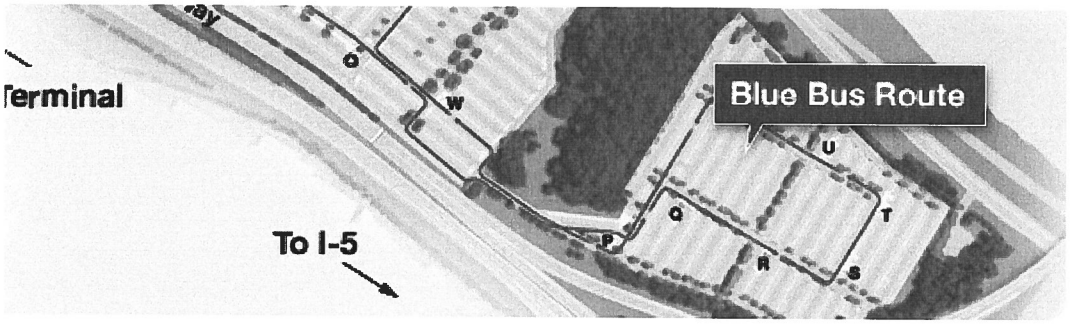
$4/Hr $30/Day

$4/Hr $24/Day

4/Hr $15/Day

ıg shuttles run regularly to the main terminal every 7-9 minutes from 4:00 a.m. - midnight, and every 15 minutes from mid

np starts & flat tire assistance
ap Accessible
ublic parking spaces
l near I-205 off of Airport Way



/ parking shuttle arrival times and live map.

lr $45/Day

CALCULATE PARKING COSTS

Entry Time

24 | 9:00 AM

Exit Time

24 | 5:00 PM

Calculate

hort-Term:	Long-Term:	Economy:	Valet:
$180.00	$144.00	$90.00	$270.00

* Calculations are provided for estimation purposes only and are based on time of entry, not entry date.

PARKING VIRTUAL TOURS

Short-Term Garage

Long-Term Garage

Cell Phone Waiting Area

Disabled Parking

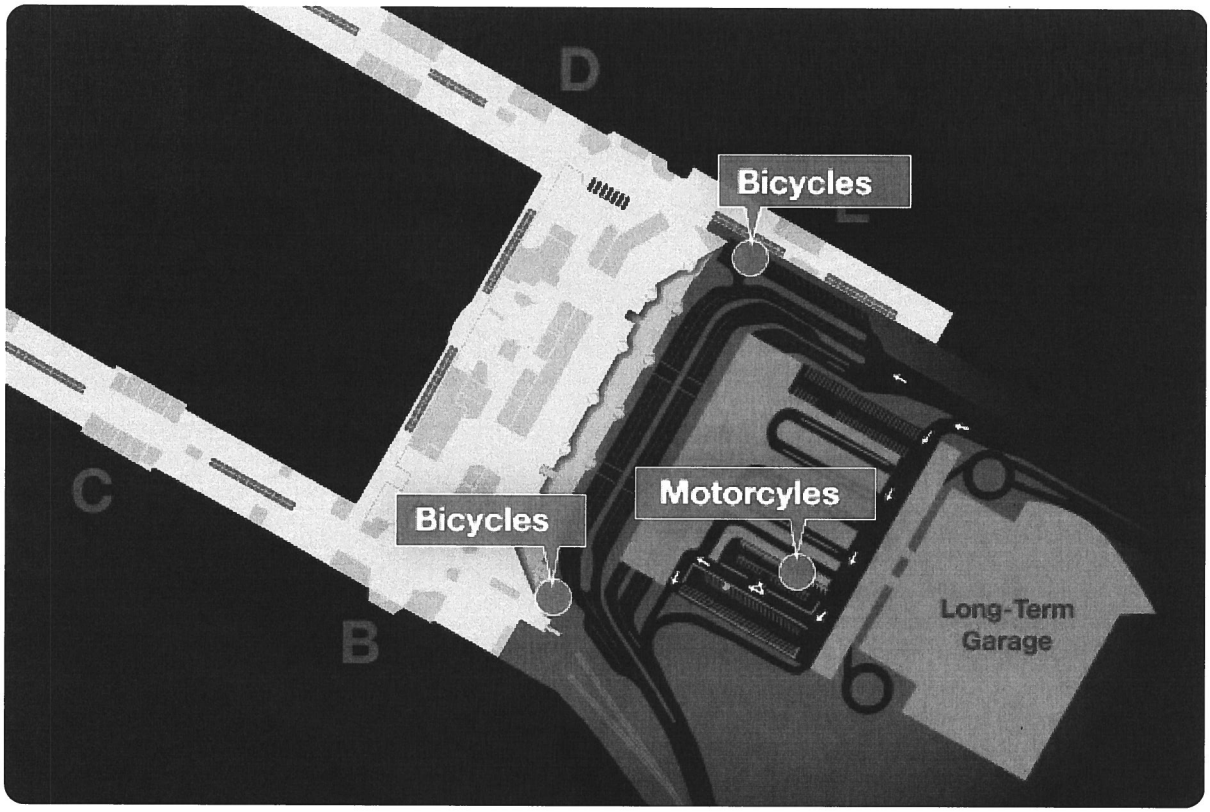
Electric Vehicles

Extended Stay

.E & MOTORCYCLE PARKING - FREE

ycle parking is available at the north end under the upper roadway and south end of the Commercial Roadv
ell marked. Follow signage on Airport Way to the free motorcycle parking area. Motorcycle parking is not av
arking garages or in the Economy or PDX employee lots.

parking is available at the north and south end of the roadway closest to the terminal building. Bicycles car
two ribbon racks located at the north end of the terminal building on the lower level and the south end of t
r the TriMet MAX Light Rail platform on the lower level. Additional bicycle parking is also available at the nor
building on the upper level. For more information, including links to trails and a map with locations, see Bic



IZED VEHICLES

503.460.4848 to determine the best parking accommodation for your oversized vehicle.

STAY CONNECTED

Current job openings at PDX.

CONTACT US

PDX Customer Service
Staffed Daily from 6 a.m. - 9 p.m.
Information & FAQs
Call or Text: Call Us 503.460.4234
Text Us
Toll Free: 1.877.739.4636

Lost & Found
503.460.4272

id International Airport (PDX) is open 24 hours, 7 days per week. Airline ticket counter and checkpoint hour

For airline information, please contact your airline directly - Airlines.

Public Records Request

DIRECTIONS