ANALYSIS

Department of Emergency Management

Cybersecurity Coordination

Analyst: Steve Robbins

Request: Acknowledge receipt of a report on the state and local cybersecurity coordination.

Analysis: The Department of Emergency Management (ODEM) provided its written report in response to the following budget note included in the budget report for SB 5701 (2024):

> *The Department of Emergency Management, in collaboration with the Department of Administrative Services, Higher Education Coordinating Commission, and Department of Justice, are directed to return to the Public Safety Subcommittee of the Joint Committee on Ways and Means during the 2025 session to report on the primary and supportive roles, responsibilities, and accountabilities of each entity related to the State's overall cybersecurity, and provide a detailed plan on how the agencies will coordinate to ensure grant funding is provided to maximize mitigation and preparedness, response, and recovery from potential cyberattacks.*

In addressing the legislative request, the multi-agency report structures its response based on the State and Local Cybersecurity Grant Program (SLCGP). The report defines the difference between a cyber emergency (unexpected and critical situation where digital systems, networks, or data are compromised) and a cyber disaster (prolonged disruption requiring extensive recover efforts). SLCGP recipients were required to develop a Cybersecurity Plan that outlines how agencies coordinate to ensure grant funding is provided to maximize mitigation and preparedness, as well as response and recover from potential cyberattacks.

The report utilizes the structure found in Oregon's Cybersecurity Plan to define cybersecurity-leading entities, their responsibilities, how SLCGP funding has been allocated, and a high-level outline of how Oregon responds to cybersecurity events.

Included in the roles and responsibilities are key participants in cybersecurity coordination at all levels of government, which include ODEM, Department of Administrative Services Enterprise Information Services (DAS EIS), the SLCGP Planning Committee, Oregon Cybersecurity Center of Excellence, Oregon TITAN Fusion Center, the federal Cybersecurity and Infrastructure Security Agency, local government entities, and the Federal Bureau of Investigation.

The SLCGP Planning Committee made recommendations for 60 projects totaling $2.8 million in Fiscal Year 2022 with an additional $6 million awarded in Fiscal Year 2023 with projects either obligated or under review.

The report then walks through the chronology of a cybersecurity event with responsibilities listed for each entity in both Executive Branch and Non-Executive Branch environments. It then breaks an event down into phases, including initial notification, pre-declaration activities, disaster declaration, ESF17 activation (referring to Emergency Support Function 17, Cyber and Critical Infrastructure Security, a section in the statewide Emergency Operations Plan), post-declaration activities, and prevention actions.

Recommendation: The Legislative Fiscal Office recommends acknowledging receipt of the report.

Oregon Department of Emergency Management
Daniel

Request: Report on State and Local Cybersecurity Grant Program by the Oregon Department of Emergency Management (OEM).

Recommendation: Acknowledge receipt of the report.

Discussion: The State and Local Cybersecurity Grant Program (SLCGP) was established in 2022 through funding from the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Law. SLCGP enables the Department of Homeland Security's Federal Emergency Management Agency (FEMA) to make targeted cybersecurity investments in state, local, tribal, and territorial government agencies to improve the security of critical infrastructure and the resilience of services provided to communities.

The budget report for Senate Bill 5701 (2024) includes a budget note directing OEM to return to the Public Safety Subcommittee during the 2025 Legislative Session to report on the primary and supportive roles, responsibilities, and accountabilities of the Agency to the State's overall cybersecurity plan. In collaboration with the Department of Administrative Services (DAS), Higher Education Coordinating Commission (HECC), and the Department of Justice (DOJ), OEM is to provide a plan detailing how each agency will coordinate to ensure grant funding is maximized for mitigation and preparedness, response, and recovery from potential cyberattacks.

OEM leads statewide collaborative efforts to protect, mitigate, prepare for, respond to, and recover from emergencies or disasters, including those impacting cybersecurity. As such, OEM's action officer coordinated with DAS-EIS, HECC, and DOJ's Titan Fusion Center in 2024 when drafting this report. OEM reconvened these partners in January 2025 to discuss, review, and rewrite the report prior to submitting it to the legislature in March. The report outlines the roles and responsibilities of each division or program within OEM, DAS, HECC, and DOJ pertinent to state cybersecurity, as well as the roles and responsibilities of relevant federal and local partners.

Oregon
Tina Kotek, Governor

Oregon Department of Emergency Management
3930 Fairview Industrial Drive SE
Salem, OR 97302
Phone: 503-378-2911
TTY: 7-1-1
www.Oregon.gov/OEM

January 24, 2025

Senator Kate Lieber, Co-Chair
Representative Tawna Sanchez, Co-Chair
Joint Committee on Ways and Means
900 Court Street NE
H-178 State Capitol
Salem, OR 97301

Dear Co-Chairs:

Nature of the Request
Budget note 7, accompanying Oregon Laws 2024, Chapter 114 (Senate Bill 5701) says:

> The Department of Emergency Management, in collaboration with the Department of Administrative Services , Higher Education Coordinating Commission, and Department of Justice, are directed to return to the Public Safety Subcommittee of the Joint Committee on Ways and Means during the 2025 session to report on the primary and supportive roles, responsibilities, and accountabilities of each entity related to the State's overall cybersecurity, and provide a detailed plan on how the agencies will coordinate to ensure grant funding is provided to maximize mitigation and preparedness, response, and recovery from potential cyberattacks.

Agency Action
The attached report responds to the budget note request.

Action Requested
The Oregon Department of Emergency Management (OEM) requests acknowledgement and receipt of the attached report.

Legislation Affected
None.

Thank you for your consideration of this request.

Best regards,

Erin McMahon
Director, Oregon Department of Emergency Management

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

LEGISLATIVE REPORT

JANUARY 2025

Executive Summary

The State and Local Cybersecurity Grant Program (SLCGP) 2025 Legislative Report responds to Budget Note 7, accompanying Oregon Laws 2024, Chapter 114 (Senate Bill 5701), which directs the Oregon Department of Emergency Management (OEM) in collaboration with the Department of Administrative Services (DAS), and Higher Education Coordinating Commission (HECC), to return to the Public Safety Subcommittee of the Joint Committee on Ways and Means during the 2025 session. The report outlines the primary and supportive roles, responsibilities, and accountabilities of each entity related to the state's overall cybersecurity. Additionally, the attached Cybersecurity Plan provides details on how the agencies will coordinate to ensure grant funding is provided to maximize mitigation, preparedness, response, and recovery from potential cyberattacks.

In 2022, the SLCGP was established through funding from the Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL). The SLCGP enables the Department of Homeland Security-Federal Emergency Management Agency (DHS-FEMA) to make targeted cybersecurity investments in state, local, tribal, and territorial (SLTT) government agencies, thus improving the security of critical infrastructure and the resilience of services provided to communities.

BUDGET NOTE 7:

> The Department of Emergency Management, in collaboration with the Department of Administrative Services, Higher Education Coordinating Commission, and Department of Justice, are directed to return to the Public Safety Subcommittee of the Joint Committee on Ways and Means during the 2025 session to report on the primary and supportive roles, responsibilities, and accountabilities of each entity related to the State's overall cybersecurity, and provide a detailed plan on how the agencies will coordinate to ensure grant funding is provided to maximize mitigation and preparedness, response, and recovery from potential cyberattacks.

TABLE OF CONTENTS

Executive Summary ***1***

Definitions ***3***

Background: Oregon Cybersecurity Plan ***3***

Roles and Responsibilities ***4***

Oregon Department of Emergency Management (OEM) 4
Department of Administrative Services (DAS)– Enterprise Information Services (EIS) 4
SLCGP Planning Committee 4
Oregon Cybersecurity Center of Excellence (CCoE) 5
Oregon TITAN Fusion Center 5
Cybersecurity and Infrastructure Security Agency (CISA) 5
Local Government Entities 5
Federal Bureau of Investigation (FBI) 6

Preparedness: Grants ***6***

Table 1: SLCGP Project Funding 7

Response ***7***

Notification of Event **7**

Pre-Declaration Activities **7**

Executive Branch Environment 7
Non-Executive Branch Environment 8

Cyber Disaster Declaration **8**

Activation of ESF17 ..... **9**

Post-Declaration Activities **9**

Executive Branch Environment 9
Non-Executive Branch Environment 10

Preventive Actions (Mitigation) ***10***

Executive Branch Environment **11**

Non-Executive Branch Environment **11**

Definitions

Cyber Emergency

A cyber emergency refers to an unexpected and critical situation where digital systems, networks, or data are compromised, causing significant disruption, damage, or risk to individuals, organizations, or governments. This can involve cyberattacks, data breaches, system failures, or any event where cybersecurity is threatened, and could result in financial loss, reputational damage, harm to critical infrastructure, or impact to government critical services that serve Oregonians.

Cyber Disaster

Unlike a cyber emergency, which may be contained and resolved more quickly, a cyber disaster often results in prolonged disruption and may require extensive recovery efforts. The impacts could be so severe that they result in the loss of life, financial ruin, or the collapse of critical services—most often on a regional scale. Examples of cyber disasters include:

- Widespread ransomware attacks that lock critical infrastructure, such as hospitals, power grids, or financial institutions, forcing them to shut down for extended periods.
- Massive data breaches that expose personal or national security information, potentially affecting millions of people or jeopardizing national security.
- Destruction of critical infrastructure (e.g., electrical grids or water treatment systems) through cyberattacks, causing long-term service outages or physical damage.

Background: Oregon Cybersecurity Plan

Under the Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law (BIL), SLCGP grant recipients must develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support plan development and identify projects for implementation using SLCGP funding. A cost share is required for all eligible entities, in either cash (hard match) or third-party in-kind (soft match). To date, FEMA has approved Oregon's request for a cost share waiver for each round of this grant. Through a partnership between OEM and the Oregon Department of Administrative Services, Office of Enterprise Information Services/Cyber Security Services (DAS-EIS/CSS), Oregon completed the required Cybersecurity Plan and established a pass-through grant program enabling state and local partners to seek funding. Pages 16 and 17 and Appendix C of the Cybersecurity Plan describe how the agencies coordinate to ensure grant funding is provided to maximize mitigation and preparedness, as well as response and recovery from potential cyberattacks.

OEM leads statewide collaborative efforts to ensure the capability to protect, mitigate, prepare for, respond to, and recover from emergencies or disasters regardless of cause, including those that impact cybersecurity. Our nation and Oregon face unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used

hardware and software, and a broad dependence on networked technologies for the day-to-day operations of critical infrastructure. Numerous Oregon communities have fallen victim to cyber incidents in recent years—Curry County's 2023 cybersecurity event is one example—necessitating support from Oregon's comprehensive emergency management response and recovery structure. The state cybersecurity office (EIS-CSS) leads cyber incident/disaster management efforts within state Executive Branch government, and in support of county and local governments after ESF 17 activation.

Roles and Responsibilities

Below is a combined overview describing the key organizations and their responsibilities regarding cybersecurity in Oregon.

Oregon Department of Emergency Management (OEM)

- **Grant Administration (SLCGP)**: OEM serves as the State Administrative Agency for Oregon and is the only entity eligible to submit SLCGP applications to DHS-FEMA. OEM ensures grant management processes comply with federal requirements and guidance.
- **Emergency Coordination**: OEM is statutorily responsible for coordinating the state's emergency management program and the state's Emergency Operations Plan (EOP). During an emergency or disaster, OEM activates the state Emergency Coordination Center (ECC) to provide a centralized location for coordination, information sharing, and resource allocation.

Department of Administrative Services (DAS)– Enterprise Information Services (EIS)

- **Cyber Expertise**: EIS (specifically through Cyber Security Services, CSS) serves as the subject matter expert in cyber-related risks and preventive measures for Oregon's Executive Branch and offers advisory support to non-executive entities. DAS-EIS will coordinate with Oregon State Police (OSP) and Oregon Department of Justice (DOJ) during cyber incidents involving data breaches.
- **Policy, Standards, and Oversight**: The State Chief Information Security Officer (CISO) is responsible for statewide information and cybersecurity standards, under ORS 276A.300. EIS/CSS follows guidance from the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and other cybersecurity organizations.
- **Program Administration (SLCGP)**: EIS is the SLCGP program administrator. The State CISO chairs the SLCGP Planning Committee, leading program administration.

SLCGP Planning Committee

- **Planning and Funding Recommendations**: Composed of representatives from cities, counties, special districts, rural, urban, and suburban communities, public health, public

safety, and critical infrastructure. The committee approves the Cybersecurity Plan, designates subcommittees, and recommends funding priorities.

- **Grant Review**: The committee designates sub-committees, reviews and recommends approval of grant funding allocations to ensure SLCGP funds are maximized to address mitigation, preparedness, response, and recovery needs.
- **Statewide Cybersecurity Plan**: The planning committee along with the CSS cyber professionals develop and review the updates of the statewide cybersecurity plan and the associated service catalog.

Oregon Cybersecurity Center of Excellence (CCoE)

- **Education and Training**: Established under House Bill 2049 (2023) with $2.5 million appropriated to the Higher Education Coordinating Commission (HECC) to operate at Portland State University. The CCoE provides cybersecurity education, awareness, and training to public, private, and nonprofit sectors.
- **Grant Program Fund**: Administers the Oregon Cybersecurity Grant Program Fund for assessment, monitoring, incident response, and competitive grants to government bodies for cybersecurity goods and services. A portion of these funds may serve as the state match for SLCGP applicants.

Oregon TITAN Fusion Center

- **Information Sharing**: Situated at the intersection of federal, state, and local law enforcement. Plays a role in sharing threat-related information between federal, state, local, private sector and tribal partners.

Cybersecurity and Infrastructure Security Agency (CISA)

- **Federal Risk Advisor**: CISA is the nation's risk advisor, helping partners strengthen their capabilities. It connects stakeholders and provides cybersecurity resources, tools, and analyses at no charge to improve the security posture of State, Local, Tribal, or Territorial Government (SLTTG) entities.

Local Government Entities

- **Maintain Local Capabilities**: Local governments maintain their own capabilities and resources for cyber disruption response. They may seek consultation and assistance from EIS, OEM, the Fusion Center, or federal partners as needed.

Federal Bureau of Investigation (FBI)

- **Investigation & Coordination**: The FBI is the leading federal agency for cyber-criminal investigations. It investigates threat actors, gathers intelligence, and coordinates information sharing with other federal, state, and local agencies.

Preparedness: Grants

Current Status of SLCGP Funds

As of July 1, 2024, Oregon's SLCGP Planning Committee recommended more than $2.8 million in grant funding allocations, and $2,461,988 in FY22 grant funds have been obligated to local partners, funding 60 projects. Two projects have been obligated using FY23 grant funds totaling $144,960. Additional FY23 projects are under review. OEM expects to obligate all $6,047,316 by Spring 2025.

Table 1: SLCGP Project Funding

Project Type	Total FY22 Investments	Total FY23 Investments
Multifactor Authentication Capability (MFA)	$165,099	$60,000
Migration to .gov Domain	$222,572	In process
Consulting/Planning	$502,491	In process
Immutable Data Backup and Recovery Testing	$857,231	In process
Vulnerability Management Services and Scanning	$142,968	In process
Albert Sensors	$76,126	In process
Advanced Endpoint Protection (AEP)	$495,501	$84,960
Total	*$2,461,988**	*In process*

By continuing to strengthen partnerships, improve resilience, and innovate cybersecurity strategies, Oregon is well-positioned to protect its communities from evolving cyber threats and ensure the uninterrupted provision of essential services.

**While $2.8 million has been obligated, $2,461,988 is the amount that has been reimbursed to subrecipients, as of this writing.*

Response

Below is a high-level outline of how Oregon responds to cyber incidents or emergencies.

Notification of Event

- **Reporting**: EIS should be notified of a cyber event as soon as possible. There is "no wrong door" for notification. EIS may receive notification directly from an agency/local entity or through the DOJ Oregon TITAN Fusion Center, OEM, the federal government partners, or the State Security Operations Center (SOC) threat-hunting effort.

Pre-Declaration Activities

Executive Branch Environment

- **OEM Role**:
  - Coordinate state response through the ECC if needed.
  - Collaborate with the State CISO to coordinate timely disaster declaration with the Governor's Office for a cyber incident, if needed

- **EIS Cyber Security Services Role**:

    - State Security Operations Center (SOC) and cyber command team begin communicating with the impacted agency.
    - Provide directions, assess threat indicators, and report findings to the State CISO.
    - Implement defensive measures (e.g., blocking networks, enhanced monitoring) based on CISO direction.
    - Coordinate with federal partners and keep OEM apprised of the cyber emergency.
    - State SOC takes command over the cyber incident, follows incident response protocols established for this purpose and manages the incident until full recovery.
- **Executive Branch Agencies**: Follow the direction of EIS/CSS.
- **Oregon TITAN Fusion Center**: Share threat-related information across relevant partners.
- **Cyber Center of Excellence (CCoE)**: No direct role in pre-declaration activities.
- **CISA**: Provide support to EIS/CSS as needed.
- **FBI**: Assist EIS/CSS upon request with investigations and threat response.

Non-Executive Branch Environment

- **OEM Role**: Coordinate or assist local governments as needed.
    - Coordinate state response through the ECC if needed.
    - Coordinate the timely disaster declaration with the Governor's Office.
    - Communicate ESF17 activations in writing.
- **EIS Role**:
    - SOC/cyber command team begins communicating with the local entity, providing consultation and threat assessment.
    - Based on CISO direction, block or secure connections to protect state assets.
    - Continue communication with local government representatives, federal partners, and OEM.
    - Establish a point of contact with the impacted local government entity and share cyber intelligence and advisories to keep them informed regularly.
    - Monitor network and assist remotely so state services can continue to be available to the residents of the local government.
    - Monitor and continuously assess to proactively prepare for ESF 17 activation.
- **Oregon TITAN Fusion Center**: Share threat-related information with federal, state, local, private sector and tribal partners.
- **Cyber Center of Excellence (CCoE)**: No direct role in pre-declaration activities.
- **CISA**: Provide support to local government entities.
- **FBI**: Lead federal agency for cyber investigations, and coordinate threat response activities.
- **Local Government**: Follow the internal Cyber Incident Response Plan.

Cyber Disaster Declaration

- **OEM Role**: Recommends declaration based on incident severity.

- **Governor's Office**: Declares a cyber disaster.
- **Cyber Center of Excellence (CCoE)**: No direct role.
- **EIS Role**: Consult with OEM and Governor's Office on threat severity.

Activation of ESF17

- **OEM Role**: Coordinate with EIS to activate ESF17 based on established criteria.
- **CCoE Role**: None for activation.
- **EIS Role (Primary Agency)**:
    - Provide cyber professional staff and IT resources for incident management and recovery.
    - Lead cyber incident command and threat eradication, including forensics.
    - Collaborate with private-sector organizations to maximize resources.
    - Execute contracts and procure services as needed.
    - Maintain trained personnel to support interagency response.
    - Identify new equipment or capabilities to address threats.
    - Coordinate with CISA, MS-ISAC, and other federal partners.
    - Analyze cyber vulnerabilities and recommend recovery measures.
    - Provide early warnings of potential threats or attacks.
    - Recommend additional cyber infrastructure partners as needed.

Post-Declaration Activities

Executive Branch Environment

- **OEM Role**: Facilitates cyber resource requests, and support recovery if requested by State CISO
- **EIS Role**:
    - Assume cyber incident command and follow state incident response protocol and manage incident activities.
    - Provide cyber professional staff and IT resources for incident management and recovery.
    - Lead or support incident command and threat eradication, including forensics.
    - Work with private-sector partners for additional resources.
    - Execute contracts and procurement as needed.
    - Maintain trained personnel for interagency emergency support.
    - Identify new equipment or capabilities for response improvement.
    - Coordinate with CISA, MS-ISAC, and other federal partners.
    - Analyze vulnerabilities and attack methods; recommend measures for service recovery.
    - Assist state agency with full-service recovery.
    - Provide early warnings of potential threats after restoration of key agency infrastructure.

    - Include additional cyber infrastructure partners as needed.
- **DOJ Oregon TITAN Fusion Center Role**: Share intelligence and threat information.
- **CCoE Role**: No direct role in post-declaration.
- **CISA Role**: Provide continued support to the local government entity.
- **FBI Role**: Lead federal investigations.
- **Oregon National Guard**: May support civil authorities under the direction of the Governor.

Non-Executive Branch Environment

- **OEM Role**:
    - Prepare communication packages, serve as liaison, and ensure threat indicators are shared promptly.
    - Activate the ECC and invite relevant cyber resources.
    - Communicate ESF17 activations in writing.
    - Coordinate resource requests and federal assistance.
    - Coordinate long-term recovery efforts once the incident is contained.
- **EIS Role**:
    - Provide cyber professional staff and IT resources for management and recovery.
    - Lead cyber incident command and threat eradication, including forensics.
    - Work with private-sector entities to maximize resource availability.
    - Execute contracts and procure goods/services as needed.
    - Maintain trained personnel for emergency response teams.
    - Identify new equipment or capabilities for improved response.
    - Coordinate with CISA, MS-ISAC, and other federal partners.
    - Analyze cyber vulnerabilities, exploits, and attack methods; recommend recovery measures.
    - Provide early warning of potential threats.
    - Recommend additional cyber infrastructure partners.
- **Fusion Center Role**: Continue to share intelligence and threat information.
- **Cyber Center of Excellence (CCoE)**: No direct role.
- **CISA Role**: Provide ongoing support, resources, and federal coordination as needed.
- **FBI Role**: Investigate threat actors and facilitate information sharing.
- **Oregon National Guard**: May support civil authorities under the direction of the Governor and Adjutant General.

Preventive Actions (Mitigation)

The following outlines ongoing preventive (mitigation) actions in both the Executive Branch and Non-Executive Branch environments to reduce the likelihood and impact of cyber incidents.

Executive Branch Environment

- **OEM Role**: Coordinates the state's emergency management program and the Oregon Emergency Operations Plan (EOP).
- **EIS Role**:
    - Per ORS 276A.300, the State CIO sets rules, policies, and standards for Executive Branch agencies.
    - EIS/CSS operates the State Security Operations Center (SOC) and provides guidance on risk reduction measures and best practices.
- **Executive Branch Agencies' Role**: Comply with rules, policies, and standards set by EIS/CSS, maintain awareness of emerging threats, and implement preventive cybersecurity measures.
- **Oregon TITAN Fusion Center Role**: Shares threat-related information with federal, state, local, private sector and tribal partners.
- **Cyber Center of Excellence (CCoE) Role**: Functions as a central resource hub (per ORS 276A.329) for strategic, educational, and remedial public cybersecurity needs, engaging multiple sectors across diverse geographic regions.
- **CISA Role**: Offers tools, assessments, and guidance (at no charge) to state agencies to help them build cybersecurity and resilience.
- **FBI Role**: Investigates cyber threats and facilitates information sharing, focusing on preventing malicious actors from executing large-scale cyber incidents.

Non-Executive Branch Environment

- **OEM Role**: Supports and advises local governments on emergency management. Coordinates statewide resources and assistance as needed.
- **EIS Role**: Advises other branches of Oregon state government, as well as federal and local government organizations, on cybersecurity best practices. Maintains the Oregon Cyber Disruption Response and Recovery (OCDR) Resource Guide for Local Government, which provides a voluntary framework for responding to cyber threats.
- **Local Government Entities**: Maintain their own capabilities and resources for cyber disruption response, incorporating voluntary frameworks like OCDR for comprehensive preparedness.
- **Oregon TITAN Fusion Center Role**: Continues threat intelligence sharing among federal, state, local, private sector and tribal partners.
- **Cyber Center of Excellence (CCoE)**: Maintains civilian resource hubs for various cybersecurity needs, ensuring strategic and educational support across public entities.
- **CISA Role**: Provides tools, guidance, and support to improve local government cybersecurity posture.
- **FBI Role**: Investigates cyber threats and malicious actors.

Looking ahead, the state remains committed to fostering collaboration, securing critical infrastructure, and maximizing the impact of federal grant funding. By continuing to strengthen

partnerships, improve resilience, and innovate cybersecurity strategies, Oregon is well-positioned to protect its communities from evolving cyber threats and ensure the uninterrupted provision of essential services.