CHARTER
Oregon Cybersecurity Center of Excellence

1. Oregon Cybersecurity Center of Excellence

Oregon House Bill 2049 (2023) (attached as **Exhibit 1**) established the Oregon Cybersecurity Center of Excellence ("Center") at Portland State University to be operated under the joint direction and control of three founding universities: Portland State University, Oregon State University, and the University of Oregon (the "Founding Members"). The Oregon Cybersecurity Advisory Council ("Council") is established within and serves as the advisory body for the Center. The Council Charter and Roster is attached as **Exhibit 1**.

2. Authority

This Charter is established by the Founding Members, and serves as the governing document for the Center, as provided in Oregon House Bill 2049 (Enrolled 2023), Section 7, Subsection 5.

As required by Oregon House Bill 2049 (Enrolled 2023) Section 7, Subsection 4, the Founding Members will enter into an Operating Agreement, which may be revised or amended from time to time, detailing the Center's administrative procedures and processes, including the provision of administrative staff support and facilities. The Founding Members will work in good faith to finalize and execute the Operating Agreement no later than December 31, 2023.

The Founding Members of the Center will review and update this Charter, as necessary, on at least a quarterly basis through June 30, 2024, and on an annual basis thereafter.

3. Membership

The Founding Members of the Center are Portland State University, Oregon State University, and the University of Oregon. The term "Operating Members" includes the Founding Members and additional Members who may join the Center at a later date, as provided below.

The primary areas of focus for each Founding Member are as follows:

PSU: Public Policy and National Security (NSA Designated Center of Academic Excellence in Cybersecurity)

OSU: Systems Security & Privacy and Cyber Operations and Services

UO: Network & Systems Security and Resiliency; Cybersecurity and Privacy; and Cyber Law and Ethics

A public university listed in ORS 352.002, or a community college operated under ORS chapter 341 may join the Center as Operating Members, and provide administrative and staff support and facilities for Center operations. This section of the Charter will be amended to include procedures for the application and approval of new Operating Members.

4. Purpose of the Center

The purpose of the Center is to supplement the activities of the State Chief Information Officer regarding cybersecurity in Oregon by coordinating, funding, or providing:

(a) Awareness, education, and training about cybersecurity and cybersecurity-related issues for public, private and nonprofit sectors

(b) Cybersecurity workforce development programs in coordination with:

- Public universities listed in ORS 352.002
- Community colleges operated under ORS chapter 341, and
- Science, technology, engineering and mathematics and career and technical education programs.

(c) Research about cybersecurity education and training methodologies

(d) Research and development of cybersecurity technologies, tools, policies, and processes, and

(e) Cybersecurity-related goods and services to public bodies, with priority given to local governments, regional governments, special districts, education service districts, school districts and libraries.

5. Duties and Responsibilities

The Center shall:

(a) Serve as the statewide advisory body to the Legislative Assembly, Governor and State Chief Information Officer on cybersecurity and cybersecurity-related issues for local governments, regional governments, special districts, education service districts, school districts and libraries.

(b) Provide a statewide forum for discussing and resolving cybersecurity issues.

(c) Provide Oregon public, private, and nonprofit sector entities with information and recommend best practices concerning cybersecurity, cyber resilience and recovery measures, including legal, insurance and other topics.

(d) Coordinate the sharing of information related to cybersecurity threats, risks, warnings and incidents, and promote public awareness and shared, real-time situational awareness among Oregon's public, private and nonprofit sector entities.

(e) Provide cybersecurity assessment, scanning and analysis, monitoring and incident response services to public bodies, with priority given to public bodies with the

greatest need for services, including local governments, regional governments, special districts, education service districts, school districts and libraries.

(f) Collaborate with public bodies to coordinate cybersecurity efforts with ongoing information technology modernization and resilience projects.

(g) Identify and participate in appropriate federal, multistate, regional, state, local or private sector programs and efforts that support or complement the Center's purpose.

(h) Pursue and leverage federal sources of cybersecurity and cyber resilience funding to achieve state goals related to cybersecurity and cyber resilience.

(i) Manage and award funds distributed to the Center for cybersecurity and cyber resilience initiatives.

(j) Encourage the development of Oregon's cybersecurity workforce by, at a minimum:

- Identifying gaps and needs in workforce programs.
- Fostering the growth and development of cybersecurity workforce development programs and career and technical education in school districts, community colleges operated under ORS chapter 341, and public universities listed in ORS 352.002.
- Assisting in curriculum review and standardization and providing recommendations to improve programs.
- Fostering industry involvement in internships, mentorship and apprenticeship programs and experiential learning programs.
- Building awareness of industry and career opportunities to recruit students into cyber-related educational tracks.

(k) Provide professional and administrative support to the Oregon Cybersecurity Advisory Council.

6. Funding and Budget Development

Oregon House Bill 2049 (2023) established three Funds in the State Treasury, separate and distinct from the General Fund. The budget report for House Bill 2049 notes that $4.9 million is to be appropriated for the Center to Public University State Programs. It is noted as a special payment – intra-agency GF transfer. Oregon Senate Bill 5506 (2023) provides the expenditure limitation (spending authority) for the legislative appropriations to these Funds. Moneys in the Funds are continuously appropriated to the Higher Education Coordinating Commission (HECC) for distribution to the Center as follows:

(a) Oregon Cybersecurity Center of Excellence Operating Fund

i. **2023-25:** $2,500,000 General Fund for startup costs for the Center.

ii. **Ongoing purpose**: Carrying out the functions and operations of the Center.

(b) Oregon Cybersecurity Workforce Development Fund

i. **2023-25:** $2,150,000 General Fund for the following programs:

- $1,000,000 for the OSU CyberClinic (ORTSOC) program
- $425,000 for University of Oregon Cyber Degree/Certificate programs
- $350,000 for the Mount Hood Community College Cybersecurity Certification Scholarship Fund
- $375,000 for the NW Cyber Camps program for high school students

ii. **Ongoing purpose:** Making targeted investments in workforce development programs designed to accelerate the growth, qualifications, and availability of Oregon's cybersecurity workforce.

(c) Oregon Cybersecurity Grant Program Fund

i. **2023-25:** $250,000 General Fund to serve as state match in support of Oregon's application for Federal Funds available through the Infrastructure Investment and Jobs Act (IIJA) and State and Local Cybersecurity Grant Program (SLCGP) through the end of federal fiscal year 2025. [**Note:** the actual amount of available federal funding and required state match will not be known until the release of IIJA SLCGP notice of funding opportunity (NOFO) for each federal fiscal year of the grant program.]

ii. **Ongoing purpose:**

- Cybersecurity assessment, scanning and analysis, monitoring, incident response and technical assistance and other cybersecurity-related goods and services to Oregon public bodies on a competitive basis with specific emphasis on serving the unmet needs of local governments, regional governments, special districts, education service districts, school districts and libraries.
- Matching funds for federal moneys related to cybersecurity received by public bodies.

(d) Initial Funding. The Center's initial 2023-25 biennium funding will be distributed as provided in **Schedule 1**, attached hereto.

(e) Emergency Board and Biennial Agency Request Budget (ARB). The Oregon Legislature has appropriated moneys to the Center via the HECC to fund the Center as a public university state program. Should the Center need to request consideration of budget, expenditure limitation, or program related requests from the Emergency Board during the legislative interim or from the Legislature during the annual or full Legislative session(s), the Center will work through the HECC as the sponsoring state agency. The Center will work with representatives from the HECC, the Department of Administrative Services Chief Financial Office, and the Legislative Fiscal Office to determine which portion(s) of Center funding will continue on an ongoing basis (as part of Current Service Level) and which portion(s) should be phased in or phased out during the biennial budget development process.

7. Strategic Planning and Reporting Obligations

(a) Strategic Plan. The Center shall work in coordination with the Council to develop a strategic plan, which must include goals and objectives for the Center. The strategic plan should be reviewed and updated no less than once every four years.

(b) Strategic Plan Reporting. The Center shall Develop and submit a report on the Center's strategic goals and objectives, operations, and funding requests for continued operations and funds administered by the Center, to the Governor and to the appropriate committees of the Legislative Assembly, in the manner required by ORS 192.245, by February 1 of each odd-numbered year. The report must identify any grants, donations, gifts, or other forms of conveyances of land, money, real or personal property or other valuable thing made to the state or the center for carrying out the purposes of the Center.

(c) Biennial Funding Reports: The Center shall submit to the Governor and to the appropriate committees of the Legislative Assembly, in the manner provided under ORS 192.245, a biennial report that summarizes specific information related to the Cybersecurity Center of Excellence Operating Fund, Cybersecurity Workforce Development Fund, and Cybersecurity Grant Program Fund, respectively. Information within the report shall include (but not necessarily be limited to): the balance of the funds; lists the deposits into and expenditures from the funds; and provide such other details as necessary regarding the operation of the funds. [**Note:** The biennial report(s) are first due no later than December 31, 2025.]

8. Staffing

(a) Center Director (PSU). The Dean of PSU's College of Urban and Public Affairs shall appoint the Center Director. The Center Director leads, coordinates, and facilitates the development and update of the Center's strategic and operations plans and the activities of the Center leadership team, comprised of the Center Director and Associate Directors, and key staff at each operating member institution. Specific Duties include the following:

- Provides management of the Center's operational activities at PSU and coordinates operational activities among and between each operating member institution (budget/finance, grant management, HR, Procurement, etc.)
- Coordinates Center outreach activities across the state by operating member institutions; conducts targeted outreach to regional governments, local governments, special districts, schools, and libraries within or near PSU's primary and extension center service territories
- Supports the Oregon Cybersecurity Advisory Council Meetings and Activities by serving as an ex-officio, non-voting member of the Council, and ensuring the Center provides professional and administrative support for the Council to perform its duties.

- Leads and coordinates with Associate Directors (OSU and UO) on the development, submission, and presentation of required reports to the HECC, the Governor, and the Oregon Legislature.

(b) Center Associate Director (OSU). The Dean of OSU's College of Engineering shall appoint the Associate Director (OSU). The Center Associate Director (OSU) actively supports and participates in the development and update of the Center's strategic and operations plans and serves as a member of the Center leadership team, comprised of the Center Director and Associate Directors, and key staff at each operating member institution. Specific duties include the following:

- Oversees the Security Operations Center Services (ORTSOC) providing services to regional governments, local governments, special districts, schools, and libraries.
- Works with the Center Director and Outreach Coordinator to conduct effective and efficient outreach to regional governments, local governments, special districts, schools, and libraries within or near OSU's primary and extension center service territories.

(c) Associate Director (UO). The Dean of UO's College of Arts and Sciences shall appoint the Associate Director (UO). The Center Associate Director (UO) actively supports and participates in the development and update of the Center's strategic and operations plans and serves as a member of the Center leadership team - comprised of the Center Director and Associate Directors, and key staff at each operating member institution. Specific duties include the following:

- Oversees the development and offering of undergraduate and graduate Cyber Degree and Certificate Programs.
- Works with the Center Director and Outreach Coordinator to conduct effective and efficient outreach to regional governments, local governments, special districts, schools, and libraries within or near UO's primary and extension center service territories.

(d) Center Staff. Staff at member institutions shall be hired or appointed by the appropriate Center Director or Associate Director(s) via the accepted human resources policies and procedures at each operating member institution and within the approved operating budget for the Center.

9. Effective Date and Duration

This agreement is effective on September 1, 2023, or the date of the last signature, whichever occurs last ("Effective Date"), and shall continue until terminated in writing by a majority of the operating members.

10. Non-Appropriation

Operating member obligations to perform duties as described within this document are conditioned upon available funding and expenditure limitation (spending authority) sufficient to allow the operating members, in the exercise of their reasonable administrative discretion, to

meet their obligations under the agreement.

11. Charter Review/Revision Process

This Charter will be reviewed and updated, as necessary, by the Operating Members on at least a quarterly basis through June 30, 2024, and an annual basis thereafter. The terms of this Charter may not be altered, modified, supplemented, or otherwise amended except by written agreement of the Operating Members.

In the event of a significant statutory change or loss/non-appropriation of funding for the Center, the Operating Members will review and, as needed, revise this document at the earliest possible time following that occurrence.

12. Authorized Representatives and Signatures

Portland State University's Authorized Representative is:

Birol Yeşilada, Ph.D., Professor and Founding Director
Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center
Phone: (503) 725-3257 | Email: yesilada@pdx.edu

Signature: _____ Date: 11/16/2023

Name: Shawn Smallman, P.h.D.

Title: Dean

Department: CUPA

DocuSigned by:
Signature: _____ Date: 11/16/2023
09BF739720C2482...

Oregon State University's Authorized Representative is:

Rakesh Bobba, Ph.D., Associate Professor
School of Electrical Engineering and Computer Science (EECS) &
Collaborative Robotics and Intelligent Systems Institute (CoRIS)
College of Engineering
Phone: (541) 737-3333 | Email: rakesh.bobba@oregonstate.edu

Signature: _____ Date: _____

Name: _____

Title: _____

Department: _____

Signature: _____ Date: _____

University of Oregon's Authorized Representative is:

Reza Rejaie, Ph.D., Professor and Head
Department of Computer Science
Phone: (541) 346-4408 | Email: reza@cs.uoregon.edu

Signature: S. Reza Rejaie S. Date: Nov. 16, 2023

Name: Greg Shabram

Title: Chief Procurement Officer

Department: Purchasing and Contracting Services

Signature: _____ Date: Nov. 16, 2023

Authorized Representatives and Signatures (Continued)

Oregon State University's Authorized Representatives are:

Rakesh Bobba, Ph.D., Associate Professor
School of Electrical Engineering and Computer Science (EECS) &
Collaborative Robotics and Intelligent Systems Institute (CoRIS)
College of Engineering
Phone: (541) 737-3333 | Email: rakesh.bobba@oregonstate.edu

Signature: DocuSigned by: Rakesh Bobba DEAC020451E6475... Date: 11/20/2023 | 22:26:17 PST

Name: Zachary Gill

Title: Director of Sponsored Programs, Award Contracting

Department: Office for Sponsored Research and Award Administration

Signature: DocuSigned by: Zachary Gill 22F9CBD4E4464AE... Date: 11/20/2023 | 14:58:58 PST

----------Continued on the Next Page ----------

ATTACHMENTS

Schedule 1. Recommended Steps for Distribution of Funding (Initial - Startup)

Schedule 2. Key Contacts

Exhibit 1. House Bill 2049 Enrolled (2023)

Exhibit 2. Draft Oregon Cybersecurity Advisory Council Charter and Roster