Mid-Year Report of the Oregon Cybersecurity Center of Excellence for the Joint Committee on Information Management and Technology, Oregon Legislature

January 4, 2024

Submitted by

Professor Birol Yesilada, Director, Portland State University
Associate Professor Rakesh Bobba, Associate Director, Oregon State University
Professor Reza Rejaie, Associate Director, University of Oregon

Background

The HB2049 (2023) established the Oregon Cybersecurity Center of Excellence (OCCOE) 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”). Governor Tina Kotek signed HB2049 into law on July 27, 2023. Whereas HB2049 stated the operations start date of OCCOE as October 1, 2023, it was not until November 16, 2023, that the three universities signed the Charter into force. The General Consuls of the founding universities are working now on the Operating Agreement for the Center.

Operations

Personnel

The General Consuls of OSU, PSU, and UO deliberated for signing the Charter of OCCOE Charter on November 16, 2023 **(Exhibit 1)**. The Oregon Cybersecurity Advisory Council (“Council”) is established within and serves as the advisory body for the Center. The Council Roster and a draft Charter are attached as **Exhibit 2**. The Advisory Council will hold its first

meeting in late January 2024. The Council will elect its chair and vice-chair, adopt the Council's Charter, and decide on the appointment of essential committees.

Portland State University appointed Professor Birol Yesilada, Director of the Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center, as Director of OCCOE at 1.0 FTE. He will be on leave from the Hatfield School of Government during his tenure as Director of OCCOE. Oregon State University appointed Dr. Rakesh Bobba, Associate Professor in the School of Electrical Engineering and Computer Science (EECS) and Co-founder of the Oregon Research and Teaching Security Operations Center (ORTSOC), as Associate Director of OCCOE at 0.50 FTE. The University of Oregon appointed Professor Reza Rejaie, Head of the Computer Science Department and Associate Director of OCCOE, at 0.50 FTE.

Four additional staff positions have been approved and advertised at PSU. They are Finance and Operations Administrator, Office Support Specialist, Senior Project Manager for Cyber Camp, Project Manager for Outreach, and Graduate Assistants. The Outreach Coordinator is at 0.50 FTE and could be increased to 1.0 FTE when additional funds become available. All the positions are 12-month appointments.

Hazel Yamada is the newest addition to the OCCOE, where she will be serving as the senior project manager, providing direction and oversight for the NW Cyber Camp program.

A part-time Program Coordinator position for OCCOE has been approved and hired at OSU. Michael Louie will support OCCOE activities from OSU at 0.5 FTE in Year 1 and 1.0 FTE in Year 2.

Workforce Development Programs at Founding Universities That Are Within OCCOE Mandate

ORTSOC: A Unique Concept

Oregon State University launched the BS Computer Science: Cybersecurity Option centered around ORTOC - the Nation's First Cybersecurity Teaching Hospital (https://ortsoc.oregonstate.edu) - this past Fall with 20+ students. It currently offers various security services to its clients, such as Security Monitoring, Security Assessment, Penetration Testing, and others.

OSU ORTSOC is serving or preparing to serve eight organizations, including two small Oregon cities, two ESDs in eastern Oregon, one Oregon county, and one Oregon community college.

With the workforce development funding from OCCOE, OSU ORTSOC is preparing to hire additional staff to expand its workforce development capacity and cybersecurity service capabilities.

For every dollar that OCCOE is putting into ORTSOC, it is leveraging up to three dollars in additional funding from federal grants, private donations, and OSU investment since its inception in 2015.

NW Cyber Camps for High School Students

This past summer, the NW Cyber Camps team hosted six summer camps across four locations, including two women-focused camps serving 120 students – 71 young men and 49 young women. The camps featured 29 guest speakers from industry and government, 23 instructors and teaching aides across the six camps, and a common investigation-based curriculum developed by OSU.

In collaboration with Portland Community College (PCC) and the Technology Association of Oregon (TAO), NW Cyber Camps hosted a networking banquet with booths/exhibits from industry, government, and academia, as well as informative panels for students and their parents/guardians. NW Cyber Camps team worked to develop coordinated proposals for the NSA GenCyber program and successfully obtained funding for three campsites for next summer. These federal grants serve as a force multiplier to the funds provided by the State, allowing OCCOE to offer more campsites across the state. OCCOE aims to host ten coordinated NW Cyber Camps across the state this Summer (2024).

OCCOE hired Hazel Yamada as Senior Project Director for Oregon Cybercamps. She started work on January 2, 2024, at the Center's PSU Office. Before joining the OCCoE, Hazel was a faculty member at PCC and Chemeketa Community College (CCC), where she taught Computer Information Systems, emphasizing cybersecurity. Hazel was a vital member of the NW Cyber Camps team in 2023. Hazel is also an experienced competitive cybersecurity coach and has coached numerous ranking collegiate cybersecurity competition teams in nationwide competitions. Before her time as an instructor, Hazel served as a cybersecurity professional within CCC and the University of Oregon's IT departments.

Non-Credit Cyber Resilience Certificate for Local and Regional Governments

During the 2023 Legislative session when OCCOE was established, PSU asked for $400,000 in two-year funding for its non-credit cyber resilience training program for local and regional governments. However, this item was removed from the Center's operating budget due to a lack of funds. PSU remedied the gap by receiving Congressional Directed Funding, sponsored by Oregon Senators Widen and Merkley, which enables us to continue the program for the current and subsequent year (**Exhibit 3**). We view this program as the foundation of expanding similar non-credit workforce training projects across Oregon through collaborative partnerships

between universities and community colleges. We plan to request funding from the Oregon Legislature as the U.S. Congressional funds run out in 2025.

New Cybersecurity Undergraduate Degree at the University of Oregon

In Fall 2023, the Department of Computer Science at the University of Oregon launched a new bachelor's degree in Cybersecurity. Upon successful completion of this program, students will be able to:

- Learn essential knowledge and up-to-date cybersecurity techniques, including fundamental security concepts and principles, applied cryptography, program security, and system and network security.
- Hone hands-on skills in cybersecurity via computer and network security lab courses and field studies.
- Be able to draw on a broad knowledge and hands-on skills of cybersecurity to design, implement, and test solutions to cybersecurity tasks.
- Understand the wide-ranging effects and interdisciplinary aspects of cybersecurity while attaining proficiency in one or multiple subdomains within cybersecurity.
- Apply and expand foundational knowledge and skills to new problem domains and emerging technologies.
- Possess effective communication and collaboration abilities and express ideas clearly and concisely, both orally and in written form.
- Adhere to ethical principles and make well-informed decisions in the field of cybersecurity.

Cybersecurity Certification Scholarship Fund

OCCOE is working with Mt.Hood and other community colleges to set up and provide scholarships from the Cybersecurity Certification Scholarship Fund established to help students pay for cybersecurity certification exams often required for cybersecurity jobs.

Outreach Activities

- Held meetings with State of Oregon Chief Information Officer (CIO) Terrence Woods and State Chief Information Security Officer (CISO) Ben Gherezgiher to coordinate how OCCOE could assist in the implementation of Oregon Cybersecurity Plan in areas HB2049 (2023) mandates as the Center's duties which overlap with the CISO's Office cybersecurity plan.

- Oregon Public Sector Cybersecurity Summit in Salem, September 27, 2023 - coincided with Governor Kotec's ceremonial signing of HB2049. Director Yesilada and David

Nevin, Director of ORTSOC, attended the summit, where Dr. Yesilada gave a presentation on the Center.

- Center leadership and Representative Nathanson participated in a panel introducing the OCCOE to the community at the Oregon Cyber Resilience Summit held at the University of Oregon on October 4, 2023.

- Professor Reza Rejaie presented on a panel, "Overbuilding? Or Futureproofing?" At the Oregon Connection Conference in Ashland, Oregon in October 2023

- Yesilada and Steve Corbato of Link Oregon discussed how OCCOE could assist in expanding Broadband in Oregon. One idea is to do a technology roadmap focusing on cybersecurity issues. Meetings every third Friday of the month. On November 16, 2023, Director Yesilada gave a presentation to the FBI at the Bureau's Portland Office on OCCOE and its activities.

- November 28-29, we attended the Cybersecurity Summit of the Umpqua Indian Development Corporation at Spirit Mountain Casino, sponsored by DruvStar. CISOs of six Indian Tribes participated in the summit.

- Attending the Special Districts Association of Oregon Annual Conference from February 9-11, 2024, to provide information to attendees on OCCOE.

- On December 8, 2023, Director Yesilada and Associate Director Bobba attended the virtual meeting of Oregon Public Universities CIOs, sponsored by PSU's CIO Ryan Bass. They presented information and answered questions on OCCOE's organization and mandate.

- Joint Press release on OCCOE by the three founding universities on January 8, 2024 **(Exhibit 4).**

- We are updating information on local governments, county governments, public libraries, community colleges, universities, and other public institutions in Oregon for their membership status with the Multi-State Information Sharing and Analysis Center (MS-ISAC).

- We plan to hold a one-day symposium on cybersecurity for local and regional governments, K12 school districts, community colleges, universities, tribal governments, public libraries, and other stakeholders during late Spring 2024. This symposium aims to provide awareness through panel discussions and enable us to gather information on cybersecurity programs across Oregon. The data will allow OCCOE to assess the state of affairs and make recommendations for furthering collaboration and development of cybersecurity educational, research, and workforce development programs in the State.

The symposium is planned at a central location that would enable the participation of representatives from rural areas.

- We started working on building a partnership between public, private, and academic institutions to better serve Oregonians in cybersecurity (awareness, education, workforce development, and better practices).

Oregon Cybersecurity Grant Program Fund

Oregon Legislature provided a $250,000 General Fund to serve as the 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 the 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.]

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 money related to cybersecurity received by public bodies.

OCCOE leadership has been meeting with the State CISO, Mr. Ben Gherezgiher, and his team on how best to coordinate our mandate. It has become clear that the $250,000 allocated as cost-share for local governments **falls very short** of the amount necessary during the current fiscal period 2023-2025. According to a letter submitted to the Co-Chairs of the September 2023 Interim Joint Committee on Ways and Means, the Oregon Department of Emergency Management (ODEM) indicated that there will be a match needed for ODEM (for grant management and administration activities), a match needed for DAS Enterprise Information Services (for statewide projects), and a match amount needed for local eligible entities (for local projects). A match waiver request has been submitted by ODEM to the U.S. Department of Homeland Security Federal Emergency Management Agency but a response has not yet been received. If the match waiver request is not approved by FEMA, IIJA SLCGP federal funding for local projects may be at risk as a funding source has not yet been identified for the local eligible entity match which was estimated to be $ 1,209,463.40 (20% of $6,047,317 available to local eligible entities during the 2023 grant year). With $250,000 in the CCOE Cybersecurity Grant Program fund, there is a funding gap of approximately $950,000 in local eligible entity match for the Federal Fiscal Year (FFY) 2023 grant year and an additional estimated funding/match gap

of between $2.5 and $3 Million combined for the remaining years of the IIJA SLCGP (FFY'24 and FFY'25) based on information provided by the State CISO.

Exhibit 1:

Oregon Cybersecurity of Excellence (OCCOE) Charter

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

Exhibit 2:

Oregon Cybersecurity Advisory Council (OCAC)

Draft Charter & Member Roster

Oregon Cybersecurity Advisory Council Charter Document

DRAFT *November 2, 2023*

Oregon Cybersecurity Advisory Council Mission/Purpose

The Oregon Cybersecurity Advisory Council (Council) serves as the advisory body for the Oregon Cybersecurity Center of Excellence (Center).

Council Duties

As the advisory body for the Center, the Council shall advise and make recommendations regarding the Center's:

- Establishment and ongoing operations;
- Cybersecurity workforce development investments and activities;
- Cybersecurity Grant Program establishment and administration; and
- Cybersecurity public awareness, education, and training activities.

In addition, the Council shall advise and provide recommendations to the Center on the:

- Development and update every four years of a strategic plan, including goals and objectives, for the Center.
- Development and submission of 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.
- The establishment and ongoing support of a statewide forum for discussing and resolving cybersecurity issues.

The Council may:

- Adopt rules, policies and procedures necessary for the operation of the Council.
- Establish subcommittees, advisory committees or other work groups necessary to assist the council in performing its duties.
- Appoint additional nonvoting members to the council.

Note: All agencies of state government, as defined in ORS 174.111, are directed to assist the Council in the performance of the Council's duties and, to the extent permitted by laws relating to confidentiality, shall furnish information and advice the Council considers necessary to perform the council's duties.

Stakeholders & Customers

- Oregonians
- Governor and Legislative Assembly
- State Chief Information Officer and State Chief Information Security Officer
- Public bodies in Oregon at federal, tribal, state, regional, local and special district levels, as well as Oregon's K-12 schools, education service districts, libraries, public universities and community colleges
- Council Membership, Subcommittees, advisory committees and work groups
- Public, Private and non-profit sector entities, regardless of physical location, that provide information and support to the Center or the Council.

Council Membership

Council membership, terms of office, and voting privileges are established in HB2049 (2023) Section 3. The Council consists of 21 appointed members (15 voting and 6 non-voting). A Council Member Roster is attached to this Charter.

Voting Members:

The Governor, after consultation with the State Chief Information Officer and the Center's director or the director's designee, shall appoint 15 voting members as follows:

1. One member who represents Indian tribes, as defined in ORS 97.740;
2. One member who represents the Association of Oregon Counties;
3. One member who represents the League of Oregon Cities;

4. One member who represents the Special Districts Association of Oregon;
5. One member who represents regional governments;
6. One member who represents the Oregon Association of Education Service Districts;
7. One member who represents the Oregon School Boards Association;
8. One member who represents the Coalition of Oregon School Administrators;
9. One member who represents public universities listed in ORS 352.002;
10. One member who represents community colleges;
11. One member who represents the office of Enterprise Information Services;
12. One member who represents a critical infrastructure sector in Oregon as defined by the Cybersecurity and Infrastructure Security Agency of the United States Department of Homeland Security;
13. One member who represents cyber-related industries in Oregon;
14. One member who represents a public sector information technology association in Oregon; and
15. One member who represents a private sector information technology or telecommunications association in Oregon.

Initially, the term of office for each voting member of the Council is as follows:

1. One-third shall serve for a term ending July 1, 2025.
2. One-third shall serve for a term ending July 1, 2026.
3. The remaining voting members shall serve for a term ending July 1, 2027.

Thereafter, the term in office for each voting member is four years, but in all cases, the member serves at the pleasure of the Governor and is eligible for reappointment.

Before the expiration of the term of a voting member, the Governor, after consultation with the State Chief Information Officer and the director of Oregon Cybersecurity Center of Excellence or the director's designee, shall appoint a successor whose term begins on July 1 following the appointment.

If there is a vacancy for any cause, the Governor, after consultation with the State Chief Information Officer and the Center's director or the director's designee, shall make an appointment to become immediately effective for the unexpired term.

A majority of the council's voting members must be geographically diverse representatives of public universities listed in ORS 352.002, local governments, regional governments, special districts, education service districts, school districts or libraries.

Non-Voting (ex officio) Members:

The non-voting (ex officio) members of the Council are to be appointed as follows:

1. The Speaker of the House of Representatives shall appoint one nonvoting member who is a member of the House of Representatives.
2. The President of the Senate shall appoint one nonvoting member who is a member of the Senate.
3. The Secretary of State shall appoint one ex officio, nonvoting member to represent the Secretary of State.
4. The State Treasurer shall appoint one ex officio, nonvoting member to represent the State Treasurer.
5. The Attorney General shall appoint one ex officio, nonvoting member to represent the Attorney General.
6. The Director of the Oregon Department of Emergency Management shall appoint one ex officio, nonvoting member to represent the Oregon Department of Emergency Management.

The term of office for each non-voting member of the Council is two years and is eligible for reappointment.

If there is a non-voting member vacancy for any cause, the appointing authority listed above shall make an appointment to become immediately effective for the unexpired term of the non-voting member.

Members of the council who are not members of the Legislative Assembly are not entitled to compensation, but the Center may reimburse a member of the Council who is not a member of the Legislative Assembly for actual and necessary travel and other expenses incurred in performing the member's official duties, in the manner and amounts provided for in ORS 292.495, from funds appropriated to the Higher Education Coordinating Commission for purposes of the council.

Members of the council who are members of the Legislative Assembly are entitled to compensation and expense reimbursement as provided in ORS 171.072.

Council Leadership

The Council shall elect one voting member of the Council to serve as Chair and one voting member of the Council to serve as the Vice Chair.

Chair – The Chair serves as the head of the Council. The Chair ensures that the Council fulfills its responsibilities, as defined in HB2049 (2023) and this Charter. The Chair works in partnership with the Center's Director to achieve the Council's and the Center's mission/purpose. The Chair has the following responsibilities:

- Approve meeting agendas and lead/conduct meetings
- Approve meeting minutes following member review
- Preview presentations/materials that are scheduled for Council review and provide feedback
- Appoint Subcommittees, advisory committees and work groups, when needed and report status of assignments to those bodies
- Promote involvement and participation of all Council members
- Respond to requests to present, speak, or testify on behalf of the Council and make appropriate assignments to Council members to meet these requests

Vice Chair – The Vice Chair (i.e. Chair-Elect) collaborates with the Chair to learn the role of the Chair, to become familiar with the Council and Center programs, and to develop and facilitate Council leadership transition. The Vice Chair assists and supports the Chair as needed and plans for their year as Chair. The Vice Chair fills in for the Chair for Council meetings if the Chair is unavailable.

Immediate Past Chair – The Immediate Past Chair provides advice and leadership to the Council regarding past practices, decisions, and other matters to assist with continuity on the Council.

The Chair, Vice Chair, and Immediate Past Chair will each serve one year in their respective offices; the Vice Chair shall automatically succeed to the Chair in the following year, and the Chair shall automatically succeed to the office of Immediate Past Chair.

The Chair may be removed from that position by the Council if, after due and proper consideration at a regular Council meeting, the Chair is determined by the Council to have been neglectful of duty or otherwise performed in a manner which was unethical or seriously detrimental to the Council's purpose or activities.

Standing Council Subcommittees

The Council may establish subcommittees, advisory committees, work groups and other bodies as deemed necessary for the purposes described in HB2049 (2023). Council subcommittees, advisory committees, work groups and other bodies do not have independent decision-making authority, but will instead provide advice, recommendations, and guidance to the Council, where decision-making authority rests.

The Council will establish the following standing subcommittees in perpetuity, and will approve the charters for each, and revisions as needed from time to time:

- Executive Committee *
- Strategy and Policy Committee
- Finance Committee
- Technology and Standards Committee
- Corporate Leadership Committee
- CISO Advisory Committee (Volunteer Senior Fellows)

*The Executive Committee is established to take actions between meetings on behalf of the Council. Any decision made by the Executive Committee must be ratified by the Council at the next full Council meeting. The Executive Committee will meet at least one time between Council quarterly meetings for agenda setting and may meet more often if urgent issues need to be addressed.

The Executive Committee is made up of the following positions:

A. Chair;
B. Vice Chair;
C. Immediate Past Chair;
D. The CCOE Director; and
E. The Chair of each Standing Council Subcommittee

Decision Making Process

A majority of the voting members of the Council constitutes a quorum for the transaction of business.

Official action by the council requires the approval of a majority of the voting members of the council.

Meetings will be conducted using Roberts Rules of Order as a guideline.

When appropriate, the Council may go into executive session per ORS 192.660 and HB2806 (2023).

Votes can be cast only by appointed voting members.

The Council may make decisions by electronic means between regularly scheduled meetings to deal with time sensitive issues, pursuant to existing Oregon statutes regarding public meetings.

Decisions will be communicated through meeting minutes, the <Insert Website and URL> website, and by formal resolutions and recommendations. Meeting agendas will be distributed in advance of full Council meetings.

Procedures and Meeting Frequency

The Council shall meet at times and places specified by the call of the chairperson or a majority of the voting members of the council.

The Council shall meet in accordance with Oregon Public Meeting Laws (ORS 192.610).

Meeting notices will be sent to Council members and posted on the <INSERT WEBSITE NAME AND URL> website.

Agenda and minutes will be forwarded in advance.

Meeting attendance will be logged.

The Center shall provide administrative and staff support, and any facilities needed for the Council to carry out its duties.

Teleconference and/or web conference capabilities will be established for regular meetings.

Certain cybersecurity documents, records, or plans protecting computers, information technology or communications systems from threat or attack are exempt from public disclosure per HB2490 (2023).

Council Member Expectations

Council members shall fulfill the following responsibilities:

- Sign a non-disclosure agreement and abide by the requirements, unless authorized by the Chair.
- Complete Center provided training on the handling and disclosure of sensitive cybersecurity information
- Attend Council meetings and actively participate
- Prepare for Council meetings
- Act on behalf of the organization they were appointed to the Council to represent
- Lead or serve on Council Subcommittees, advisory committee as requested

Council Guests

Council Guests will adhere to the following:

- Sign a non-disclosure agreement and abide by the requirements, unless authorized by the Chair.
- Attend Council meetings when requested, adhering to meeting guidelines with participation during defined portions of the meeting as specified in the agenda or requested by the Chair

Communication Plan Elements

- Council meetings are open to the public and subject to Public Meetings laws
- Regular reports will be made to stakeholders on progress
- Periodic solicitation of stakeholder input will be made
- Reports made to State Chief Information Officer, Governor and Legislature
- All information about Council activities is updated regularly on the <Insert Name and URL of Website> website

Charter Review/Revision Process

This Charter shall be reviewed (and revised as appropriate) by the Council by January 31st of each odd numbered year.

Revisions to the Charter shall be affirmed via the Decision-Making Process outlined within the Charter.

Attachments -

- HB2049 Enrolled (Laws of 2023)
- Oregon Cybersecurity Advisory Council Membership Roster (November 1, 2023)
- Version History and Document Review

Version History

NUMBER	CHANGE DATE	AUTHOR	SUMMARY OF CHANGE

Document Review

Name	Title	Reviews/Approves	Date

Oregon Cybersecurity Advisory Council - As of November 1, 2023 (TERMS)

House Bill 2049 (2023) established the Oregon Cybersecurity Advisory Council as the Advisory Body for Oregon's Cybersecurity Center of Excellence. A majority of the council's voting members are geographically diverse representatives of public universities listed in ORS 352.002, local governments, regional governments, special districts, education service districts, school districts and libraries. The Council is comprised of six (6) non-voting, and fifteen (15) voting member representatives as follows:

	Name	Organization	Representing	Term Start	Term End
	Non-Voting Members				
1	Rep. Nancy Nathanson (Appointed September 8, 2023)	Oregon Legislative	Oregon House of Representatives	October 1, 2023	September 30, 2025
2	Sen. Aaron Woods (Appointed September 26, 2023)	Oregon Legislature	Oregon Senate	October 1, 2023	September 30, 2025
3	Chris Molin, CIO (Appointed August 16, 2023)	Oregon Secretary of State	Oregon Secretary of State	October 1, 2023	September 30, 2025
4	Michael Kaplan, Deputy State Treasurer (Appointed September 6, 2023)	Oregon State Treasury	Oregon State Treasurer	October 1, 2023	September 30, 2025
5	Richard Rylander, CIO (Appointed August 28, 2023)	Oregon Department of Justice	Oregon Attorney General	October 1, 2023	September 30, 2025
6	Curtis Peetz, Response Planner (Appointed August 28, 2023)	Oregon Department of Emergency Management	Oregon Dept. of Emergency Management	October 1, 2023	September 30, 2025

----------See Voting Members on Next Page ----------

Oregon Cybersecurity Advisory Council - As of November 1, 2023 (TERMS)

	Name	Organization	Representing	Term Start	Term End
Voting Members					
1	Richard Rader, Chief Technology Officer	Cow Creek Band of Umpqua Indians - Umpqua Indian Development Corporation/Seven Feathers Casino & Resort	Oregon Indian Tribes	November 1, 2023	June 30, 2026
2	Robin Mayall, Director - Department of Information Services	City of Eugene, Oregon	League of Oregon Cities (LOC)	November 1, 2023	June 30, 2026
3	Greg Hardin, Cybersecurity Specialist/Systems Architect	CIS (Citycounty Insurance Services)	Association of Oregon Counties (AOC)	November 1, 2023	June 30, 2026
4	Frank Stratton, Executive Director	Special Districts Association of Oregon (SDAO)	Special Districts Association of Oregon (SDAO)	November 1, 2023	June 30, 2027
5	Brenda Wilson, Executive Director	Lane Council of Governments (LCOG)	Oregon Regional Governments	November 1, 2023	June 30, 2027
6	Rachel Wente-Chaney, Chief Information Officer	High Desert Education Service District	Oregon Association of Education Service Districts (OAESD)	November 1, 2023	June 30, 2027
7	Lori Sattenspiel, Director of Legislative Services	Oregon School Boards Association (OSBA)	Oregon School Boards Association (OSBA)	November 1, 2023	June 30, 2026
8	Glen Szymoniak, Superintendent	Klamath County School District	Coalition of Oregon School Administrators (COSA)	November 1, 2023	June 30, 2025
9	Gary Robert Lomprey, CISSP Assistant Professor - Cybersecurity	Oregon Institute of Technology (Oregon Tech)	Oregon Public Universities	November 1, 2023	June 30, 2025
10	Laura Boehme, CIO @ COCC	Central Oregon Community College (COCC)	Oregon Community Colleges	November 1, 2023	June 30, 2025
11	Ben Gherezgiher, State Chief Information Security Officer	State of Oregon - Office of Enterprise Information Services (EIS)	Office of Enterprise Information Services (EIS)	November 1, 2023	June 30, 2027
12	Janna Sondenaa, Program Manager - Security Awareness	Portland General Electric (PGE)	Oregon critical infrastructure sector	November 1, 2023	June 30, 2026
13	Dominic Perez, Chief Technical Officer	PacStar/Curtiss-Wright Defense Systems	Oregon cyber-related industries	November 1, 2023	June 30, 2025
14	Jessica Chastain, IT Director Klamath County	Oregon Association of Government IT Management (OAGITM)	Oregon public sector information technology association	November 1, 2023	June 30, 2025
15	Skip Newberry, President and CEO	Technology Association of Oregon (TAO)	Oregon Private sector information technology or telecommunications association	November 1, 2023	June 30, 2027

Exhibit 3:

Building Cyber Resiliency

PROFESSIONAL CERTIFICATE IN BUILDING CYBER RESILIENCE

12-WEEK PROGRAM FOR PUBLIC SERVICE LEADERS

ABOUT THIS PROGRAM

Understanding cybersecurity risk is an essential first step in protecting data and ensuring organizational resiliency in the event of a cyber-attack or natural disaster. Cyber risks can take the form of technical or physical threats or vulnerabilities, regulatory compliance requirements, financial loss, data loss, or reputational harm.

This program is highly collaborative and will use a cohort-based case study approach to learn about common cyber risks; how to identify, assess, and communicate cyber risk; and how to conduct the first step in mitigating threats through a risk assessment. A deep technical background isn't required, and technical concepts will be explained through the course of 12 weekly sessions. Program staff will work with participants to create a unique shared learning experience that is approachable for non-technical practitioners

WHAT YOU WILL LEARN

- How to create and implement a comprehensive cyber risk assessment program for your organization
- How to leverage internal and external collaboration to enhance risk management
- The impact of cyber threats and vulnerabilities on organizational resiliency
- How issues such as privacy, legal and regulatory frameworks and compliance, social and geopolitical impacts, national security and evolving technologies can impact an organization's cyber risk and security posture
- The importance of identifying and mitigating risks from vendors and other external partners
- Sessions delivered in a virtual format with live instructors & student interaction every Friday alongside online lessons to be completed each week
- How to enhance eligibility in acquiring federal grants in cybersecurity

WHO SHOULD ATTEND

Portland State University's Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center is proud to offer, at no cost, this certificate in risk-based organizational cybersecurity resilience. Whether you are an experienced cybersecurity professional or in a role that intersects cybersecurity risk management, this certificate program is designed for you. Specifically, you must work for a public sector organization, including state, local, special districts, school districts, and tribal governments or organizations. Examples of positions or roles that will benefit from this certificate program are:

- Information, financial, and operations officers
- Security officers
- Administrators and staff
- Information technology (IT) director/manager
- Disaster recovery and business continuity
- Vendor management
- Contracting and procurement

PROGRAM INFORMATION

START DATE

January 19th - April 5, 2024 (live sessions on Fridays, 9:00 am - 10:30 am)

COST

No cost for selected participants

Apply by December 8th, 2023 for consideration

Portland State
Mark O. Hatfield Cybersecurity
& Cyber Defense Policy Center

ABOUT THE CENTER

The Mark O. Hatfield Center for Cybersecurity is an NSA/DHS National Center of Academic Excellence in Cyber Research.

INSTRUCTORS

Your instructors will be experts in cybersecurity, collaboration, and local government. This unique combination of expertise and practical experience will help ensure an accessible and highly impactful program.

MARGARET E. BANYAN, PH.D.

Margaret E. Banyan, Ph.D serves as a Research Professor for land use planning, strategic planning, organizational design and development, and sustainability planning. Dr. Banyan is extensively involved in organizational and strategic planning in a variety of national, regional, and local efforts. She has worked with a wide range of local governments, nonprofit organizations, and special districts conducting policy and organizational studies. She has published in Public Administration Review, Administrative Theory and Praxis, the Encyclopedia of Governance, and authored several individual and joint book chapters.

Dr. Banyan has significant experience in both the public and private sectors, including serving as a Professor at Florida Gulf Coast University, Senior Fellow for Portland State University, a Senior Planner, Special (Fire) District Administrator, Coordinator for the Center for Public Participation, and Hatfield Scholar at Portland State University. She has designed and implemented innovative projects, collaborative research initiatives, and multi-jurisdictional planning efforts; including cybersecurity studies, strategic plans, comprehensive land use policies, community plans, economic development initiatives, health impact assessments, citizen surveys, focus groups, and needs assessments.

Dr. Banyan holds a Ph.D. in Public Administration and Policy from Portland State University, a Master of Public Administration from Portland State University, and a Bachelor of Science, History, from the University of Oregon.

RONALD BUCHANAN, M.A.

Ronald Buchanan is Chief Information Security Officer (CISO) for the St. Charles Health System in Bend, Oregon. Prior, he was CISO for the state of Washington and Chief Information Risk Officer and Director, Information Security & Privacy Office, for Oregon's Department of Human Services and the Oregon Health Authority. Before joining the state of Oregon, Ron consulted with Pearson VUE to build their global special investigations and threat analysis program identifying and mitigating technical and physical threats to Pearson VUE's intellectual property. As a consultant for the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Division, Ron was a lead author for the CJIS Security Policy resulting in a national risk-based and technology agnostic framework for protecting Criminal Justice Information. Additionally, he served as a civilian Supervisory Special Agent with the Air Force Office of Special Investigations focused on cybercrime and counterintelligence investigations and operations in the US, Europe, and Asia.

CONTACT

Sullivan Swift, suswift@pdx.edu

Learn more at:
pdx.edu/hatfield-school/professional-certificate-building-cyber-resilience

Portland State
Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center

Exhibit 4:
Press Release
Oregon Cybersecurity Center of Excellence

Press Release

Joint Cybersecurity Center formed at Oregon's Three Largest Universities

(Corvallis, Eugene and Portland, Ore – for immediate release) Cybersecurity experts from the state's three largest research universities have joined together to launch the Oregon Cybersecurity Center of Excellence with the goal of improving Oregon's resilience to cyberattacks. The Center, which will serve as an advisory body to the Governor and the State Legislature, will also help coordinate cybersecurity workforce development, education, awareness, and training across the state, as well as focusing on the unmet needs of regional and local government agencies, special and school districts, and libraries.

The Center, housed at Portland State University (PSU) and operated jointly by PSU, Oregon State University (OSU), and University of Oregon (UO), was created by the passage of HB 2049, which was signed into law by Governor Tina Kotek in July. The bill, co-sponsored by Representative Nancy Nathanson of Eugene and Senator Aaron Woods of Wilsonville, represents years of work to garner enough support to gain passage.

"Cyberattacks hit public agencies, private businesses, and individuals daily. Malicious actors are demanding ransom payment in exchange for access to stolen data," said Representative Nathanson, when describing the need for a Center. "Oregon school districts, cities, and businesses aren't just vulnerable – they are being attacked."

"HB 2049 marks a significant stride in fortifying Oregon's digital defense by establishing the Cybersecurity Center of Excellence, a hub for enhancing cybersecurity expertise and resources across public, private, and educational sectors. The center will boost Oregon's cybersecurity workforce and help fortify Oregon against evolving digital threats," said Senator Woods.

Birol Yesilada, a Professor at PSU and Director of the Mark O. Hatfield Cybersecurity and Cyber Defense Center there, will serve as the Center's first Director. Yesilada noted that activities coordinated by the Center will measurably improve the security, privacy, and resiliency of cyberspace in Oregon. He stated that many organizations across the state, including the League of Oregon Cities, the Oregon Association of Counties, the Technology Association of Oregon, and others were involved in making this Center a reality. "The opportunity for having such a profound societal impact and working with all these stakeholders make our involvement in the Center uniquely exciting," Yesilada said.

Having three major universities join to host such a Center is unusual. Reza Rejaie, Professor and Department Head of Computer Science at UO, offered that it is a good role for the schools. "Universities are uniquely positioned to establish or extend relationships with various

stakeholders, and collectively offer the required expertise and experiences to support, coordinate, and execute wide range of envisioned activities to address Cybersecurity challenges across the state." Rejaie will serve as an Associate Director of the Center.

"It is also helpful that the three schools, and the people involved, work incredibly well together—it is a great team," said Rakesh Bobba, Associate Professor in Electrical Engineering and Computer Science at OSU, who joins Rejaie and Yesilida at the Center as an Associate Director. "I'm especially excited by the workforce development opportunities in cybersecurity the Center will help create, and the direct impact this will have on improving Oregon's cybersecurity posture," he said.

Since the bill's signing in July, the three universities have worked together to develop a charter for the center, which was signed into effect in November. Center activities are anticipated to begin mid-January.

###

For more information:

Birol Yesilada, yesilada@pdx.edu, (503) 725-3257
Reza Rejaie, reza@cs.uoregon.edu, (541) 346-0200
Rakesh Bobba, Rakesh.Bobba@oregonstate.edu, (541) 737-3333