Oregon Cybersecurity Center of Excellence

Joint Legislative Committee Information Technology and Management Meeting

September 10th, 2026

Presenters

Birol Yeşilada, Director

Reza Rejaie, Associate Director

Rakesh Bobba, Associate Director

Oliver Grant, Finance and Operations Manager

Agenda

- [x] Water Districts Discussion
  - Oregon Cyber Threat Assessment
  - Risk Heat Map
  - Cyber Threat Pathway: Water Infrastructure
  - RISK Clinic
  - Cyber Oregon Collaborative
- [x] OCCoE Updates
  - Accomplishments
  - MHCC Scholarship Fund
  - Financial Performance

Water Districts Discussion

Oregon Cyber Threat Assessment

From Ransomware to State Actor Pre-Positioning

2020 - 2025

Cybercrime Dominance

The baseline threat environment was defined by financially motivated actors.

- Crypto scams and extortion
- Business Email Compromise (BEC)

2024 - 2026

State Actor Escalation

A significant pivot toward foreign state adversary activity and sophistication.

- AI-enabled fraud
- Identity exploitation
- Advanced persistence

Strategic Shift

Targeting Infrastructure

Critical utility and physical infrastructure have become the primary threat focus.

- Operational tech risk
- Water and energy sectors
- Hybrid tactical attacks

Current Status

Pre-Operational Phase

Oregon is actively in a pre-operational threat phase with foreign adversaries.

- System reconnaissance
- Pre-positioning implants
- Strategic leverage goals

2026 Risk Heat Map (Sector*Actor*Probability)

Probability × Impact Matrix (Oregon 2026-2027 Outlook)

Sector	Cybercrime	China (State)	Iran (State/Proxy)	Russia/Hybrid	Overall Risk
Government	🔴 High	🔴 Very High	🟡 Medium	🔴 High	🔴 High
Healthcare	🔴 High	🟡 Medium	🔴 High	🟡 Medium	🔴 High
Water Systems	🟡 Medium	🔴 Very High	🔴 High	🔴 High	🔴 Critical
Energy Grid	🟡 Medium	🔴 Very High	🟡 Medium	🔴 Very High	🔴 Critical
Education/Research	🟡 Medium	🔴 High	🔴 High	🟡 Medium	🔴 High
Private Vendors	🔴 High	🟡 Medium	🔴 High	🟡 Medium	🔴 High

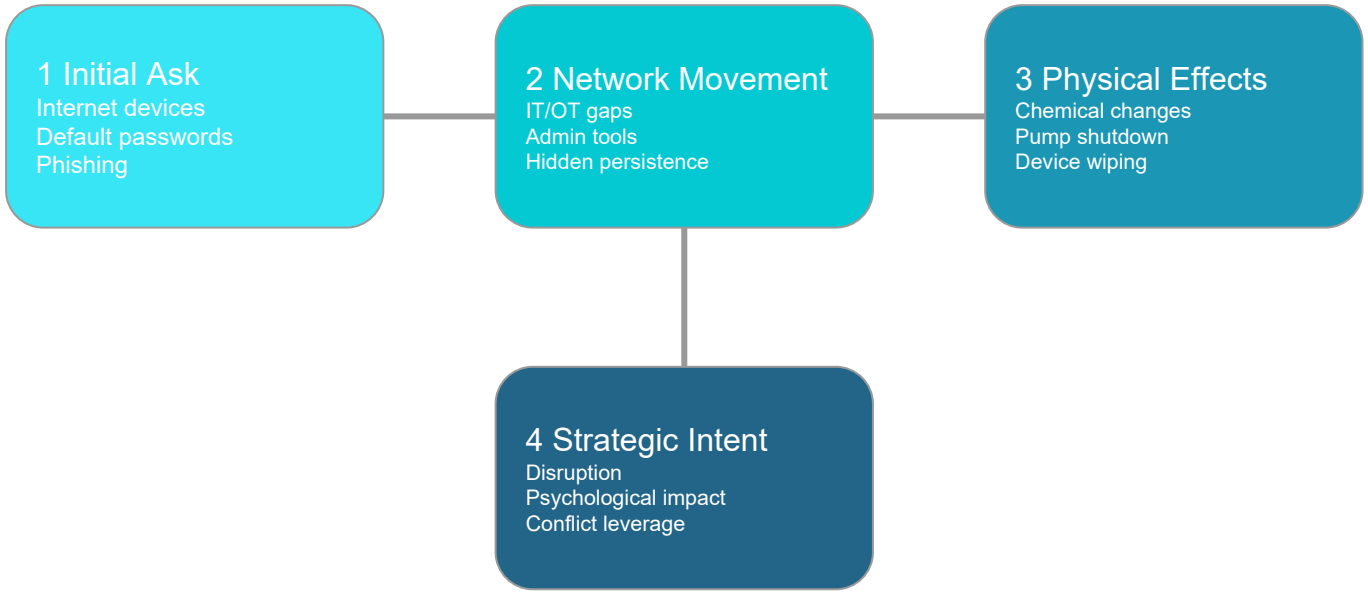
Key Insight:

•Highest risk concentration:

- Water + Energy = **State actor battlespace**
- Healthcare + Vendors = **Hybrid disruption layer**

Do Not Cite Without Permission - ©Birol Yesilada

Cyber Threat Pathway: Water Infrastructure (Executive Overview)



Key takeaway: Cyber access to water utilities can rapidly translate into real-world infrastructure disruption.

- The Oregon Health Authority's Drinking Water Services program regulates roughly 3,450 public water systems in Oregon, and includes municipalities, private systems, schools, and mobile home parks — far broader than "districts."
- **No one has actually surveyed Oregon's water districts and sorted them into SCADA/OT capability tiers.**
- **AWIA (America's Water Infrastructure Act)** does have a real, official categorization, but it is population-based, not capability-based.
- **OHA/EPA SDWIS** classifies by population-served size bands (very small, small, medium, large, very large) for regulatory/monitoring purposes — again, population, not cyber capability.

RISK Clinic Update—Summary

University of Oregon | CISA CPG assessments for up to 100 Oregon water districts | SLCGP 2024–2025 (CY23-119) | 09/03/26

178	33	51	76
Districts scoped	Invited Leads	Awaiting Callbacks	Call Queue

What is it?

- UO-led clinic delivering state-approved CISA CPG assessments to water/wastewater facilities serving major population areas
- Works alongside OCCoE and the UO Teaching SOC (Computer Science)
- Compliance team: Leland VanBrunt (Senior IT Compliance Analyst), Andy Preising (IT Compliance Analyst)

Year 1 accomplishments

- Contract finalized; equipment and storage procured
- Backend tracking, processes and documentation built
- Student assessors hired and trained
- In/out-of-scope tiers defined with CISA and Oregon CISO Office; pamphlets distributed statewide

Next 10 months

- Webinars Sept 14, 21 and 24, 2026
- Four-step process: reach out → intro call → 1–2 hr guided CPG walkthrough (no prep) → plain-language findings
- Prioritized reports give district boards evidence for grant requests

Cyber Oregon Collaborative

Piloting new avenues to extend the reach of the Center

Cyber Ambassadors

- Graduates from the *Certificate for Building Cyber Resilience* become **Cyber Ambassadors** within their communities
- **Statewide reach** - Grads live and work across the state
- **Knowledgeable and experienced** OCCoE instructors develop curriculum

Applying for NSF Grant

Cyber Mentor Alliances

- NW Cyber Camp students provided free Fortinet training
- Successful completion of course would lead to in person problem solving workshop
- Networking opportunity for students and future employees for organization

Applied for RAMPs Grant

Cyber Corps

- Partnership with Washington Emergency Management Division as they stand up a Cyber Incident Response Team (CIRT)
- Ideally, proactive assessments and response to cybersecurity incidents
- OR National Guard also performs assessments and would be a natural fit

OCCoE Updates

Accomplishments

Workforce Development

Over 100 individuals participated in Building Cyber Resilience programs*

*An additional 312 participants from 2022-2025

49

Employees Trained

in Certificate in Building Cyber Resilience for Local Govt, Special Districts, School Districts, & Tribes

24

SLTTs Participated

in targeted Tabletop Exercises to test active response capabilities, with more coming this fall

"The most important component in a course are the people in it—the teachers, students, staff. Second is the quality of the teachings. This course was excellent on both."

- Cybersecurity Education for **Tribal participant**

18+

Certificate Alumni

engaged via structured Information Sharing Monthly Meetings

80

Tribal Members & Employees*

representing 13 tribes across 3 states in Cybersecurity Education

*Additional 21 served in 2025

"I feel I have gained so much awareness and information for me, I would be an asset to our organization when it comes to planning and research needed especially in the communication piece, which role/players do what, follow-up. We all play a role in cyber security regardless our positions. Thank you for this opportunity to be part of this class."

- Certificate program participant

Accomplishments

Workforce Development

- **ORTSOC - a year long practicum**
  - **148 students** trained to date (91 in AY 25-26)
  - **87+ students enrolled** for AY 26-27
  - **Ecampus offering launches** in Fall 2026

"We need professionals who can contribute from day one: respond under pressure, communicate with impacted customers, understand how a real SOC operates. ORTSOC delivers that through hands-on experience."

- Bryce Schroeder, VP of Customer Security & Trust for ServiceNow

"ORTSOC has established itself as the state's flagship program for developing practicing security professionals. By combining academic rigor with operational experience, the program is building Oregon's next generation of security leaders while actively defending the state's critical infrastructure. As the program expands to serve more organizations each year, the impact grows exponentially."

- Steve Person, Chief Information Security Officer and Vice President of Infrastructure and Operations at Cambia Health Solutions

Accomplishments

Workforce Development

- **TSOC - UO's newly launched teaching SOC**
  - **Offered the "CyberOps I" course every term**
  - **Trained 26+ students** over the past 9 months
  - **Expanded the TSOC curriculum** with new CyberOps II and III courses
  - **Developing a CyberAI Lab** adjacent to the TSOC to support hands-on learning

UNIVERSITY OF OREGON

Teaching Security Operations Center

"Although my time with the TSOC was relatively short, the experience significantly expanded my technical capabilities and provided meaningful hands-on experience that contributed to my growth as a cybersecurity professional. "

- TSOC Student

Accomplishments

Workforce Development

Nurturing Inclusive Cybersecurity Education (NICE) for high school teachers and students.

42

Teachers Attended

32 or 40 hour cybersecurity professional development workshops to teach a cybersecurity course

247

Students Engaged

through in-school field trips bringing cybersecurity educational pathway information to them

223

Students & Adults Visited

the UO campus for customized tours of cybersecurity programs

29

Students Participated

in DUCKS Cyber Competition asynchronously from 10 high schools

"This workshop was absolutely critical to helping me ramp up my cybersecurity skill set. I feel confident offering the class for the first time at my high school."

- *NICE Workshop Teacher Participant*

Accomplishments

Workforce Development

- **NW Cyber Camps - Summer 2026**
  - **191 middle and high school campers**
  - New and expanded curriculum
  - 9 different camps around Oregon; added SOU this year
  - Supported in part by foundation & industry partners

Accomplishments

Services and Advisory

ORTSOC

- Currently serving **20 Oregon organizations** and growing
- Performed **12 security assessments** and **12 penetration tests** last academic year in addition to SOC services

Oregon State University

TSOC

- Currently serving 3 Oregon public entities
- Actively expanding outreach

University of Oregon
Teaching Security Operations Center

LGP Special Districts

- Initiative started in July 2026
- Successfully engaged with 4 special districts as of now

Oregon State University

SLCGP Risk Clinic

Previously covered in detail.

University of Oregon

Accomplishments

Public Awareness and Outreach

- State and federal agency partnerships to deliver cybersecurity resilience workshops and table-top training exercises called the "**Pacific Disruption Series**" -partnered with CISA, FBI, TSA, EIS, OEM, Titan Center, OR National Guard, OEDI.

Research Innovation and Development

- Research results briefings on critical infrastructure (CI) with the Governor, legislative committees, department leaders, federal agencies, BPA, and other CI stakeholders

MHCC Scholarship Fund

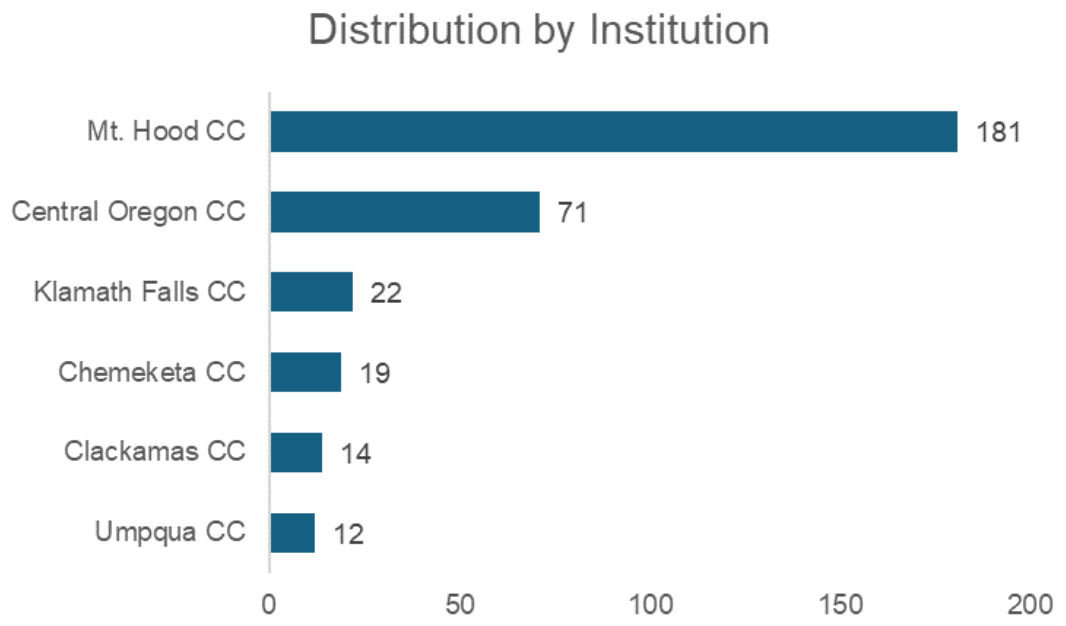
Vouchers distribution has been increasing since launch

319
Vouchers issued

$96K
Dollars spent

$253K
Remaining budget

6/30/27
Contract expires

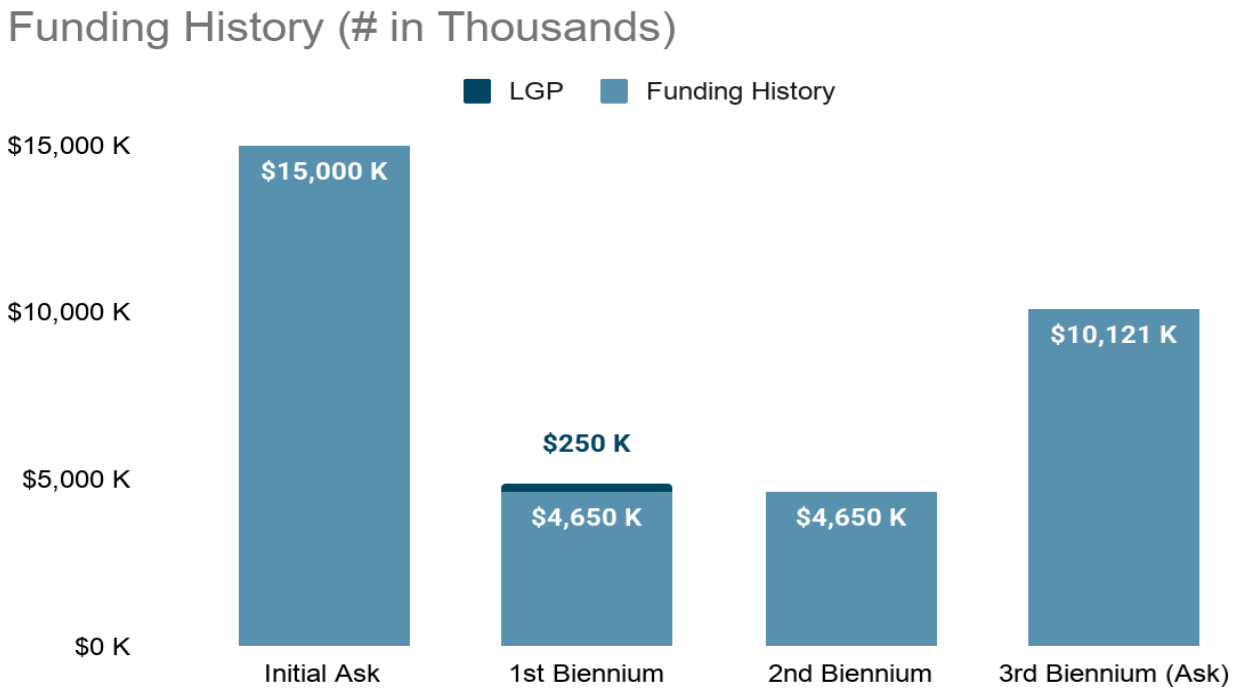


96%

of Certificates are CompTIA, global certification that establishes the essential skills required for core security functions and a career in IT security.

Financial Performance

OCCoE has been a responsible steward of the State's investment and has delivered positive outcomes; with expanded funding, it could fully achieve its broader mandate.



1ST BIENNIUM

3X

REVENUE GROWTH

Amplified Center's funding by tripling the investment the state has made through various sources.

GRANT	SOURCE	AMOUNT
NW Region Cybersecurity Risk Management and Roadmapping for Smart Grid Critical	NSA	$2,000K
GenCyber Camp 2023	NSA	$250K
Cybersecurity Resilience Training	DOE	$600K
GenCyber Camp 2024	NSA	$552K
Workforce Ready Round III: Technology (Tribes)	HECC	$604K
NICE: Nurturing Inclusive Cybersecurity Education	HECC	$500K
SFS CyberCorps Scholarship Program	NSF	$4,800K
CyberService Academy Scholarship Program	DOD	$76K
TOTAL		**$9,382K**

2ND BIENNIUM

Will continue to seek additional funding but early results indicate that funds may not be as available as in the past.

GRANT	SOURCE	AMOUNT	STATUS
GenCyber (UO)	NSA	$75K	**Declined**
GenCyber (OSU)	NSA	$90K	**Declined**
PRISM (OSU)	ARL	$700K	**Declined**
CyberService Academy Scholarship (OSU)	DOD	$130K	Awarded
CICI (OSU, UO)	NSF	$1,475K	Awarded
CyberAI Innovation (UO)	NSF	$500K	Pending
CyberAI Corps (OSU, UO)	NSF	$5,000K	Pending
SaTC2.0 (PSU)	NSF	$600K	Pending
Ramps-01 (TAO)	NIST	$200K	Pending
AI-COP (UO)	NSA	$954K	Pending
TOTAL		**$9,724K**	

Thank You