



---

# **Oregon Cybersecurity Advisory Council**

## *Cyber Center of Excellence Plan - Update*

---

March 2019

# Testimony By

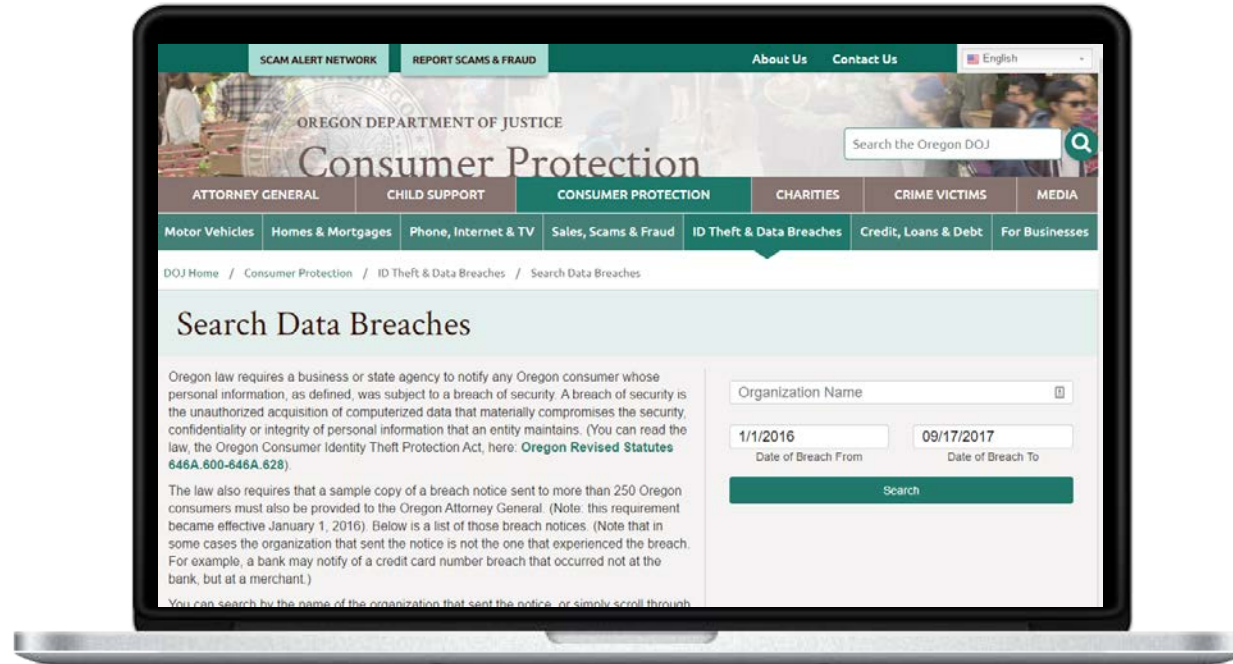
---

- Kerri Fry  
SVP Operations and Finance, InfoGroup Northwest (IGNW)  
Chair, Oregon Cybersecurity Advisory Council
- Charlie Kawasaki, CISSP  
CTO, PacStar  
Vice-Chair, Oregon Cybersecurity Advisory Council  
Board Member, Technology Association of Oregon  
Board Member and Executive Council, OSU Industry Advisory Board



# Oregon Cyber Breaches

279 companies reported breaches since Jan 1, 2016



As of 2/24/19

<https://justice.oregon.gov/consumer/DataBreach>



## Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share Embed

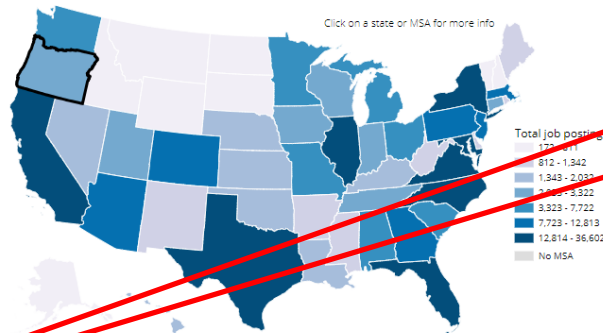
All Data Public Sector Data Private Sector Data

States

Metro Areas

Total Job opening

Search State



Oregon  
2,911 unfilled positions

## Oregon

### TOTAL CYBERSECURITY JOB OPENINGS

2,911

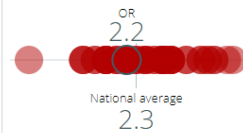
### TOTAL EMPLOYED CYBERSECURITY WORKFORCE

6,475

### SUPPLY OF CYBERSECURITY WORKERS

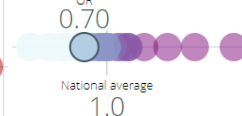
Very Low

CYBERSECURITY WORKFORCE  
SUPPLY/DEMAND RATIO



### GEOGRAPHIC CONCENTRATION

Low  
LOCATION QUOTIENT



### TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Consultant
- Vulnerability Analyst / Penetration Tester
- IT Auditor
- Software Developer / Engineer
- Systems Engineer
- Cyber Security Architect



# Oregon Cybersecurity Advisory Council

## Voting

Kerri Fry, IGW

Charlie Kawasaki, PacStar

Michael Gutsche, Microfocus International

Andrew Plato, Anitian

Tom Quillin, McAfee

Prof. Rakesh Bobba, Oregon State University

Dennis Tomlin, Multnomah County

Mike Wells, Oregon Department of Justice

## Non-Voting

Ron Talwakar, Eclysium

Kris Rosenberg, Riperia

Theresa Masse, Port of Portland

Margaret Banyan, PhD, Portland State University

Megan McKenzie

McKenzie Worldwide PR

*Council Secretary (Non-Voting)*

## Executive Sponsors

Terrence Woods, Oregon State Chief Information Officer

Annalise Famiglietti, CISM, Oregon Interim Chief Information  
Security Officer

David McMorries, State of Oregon

Skip Newberry, Technology Association of Oregon

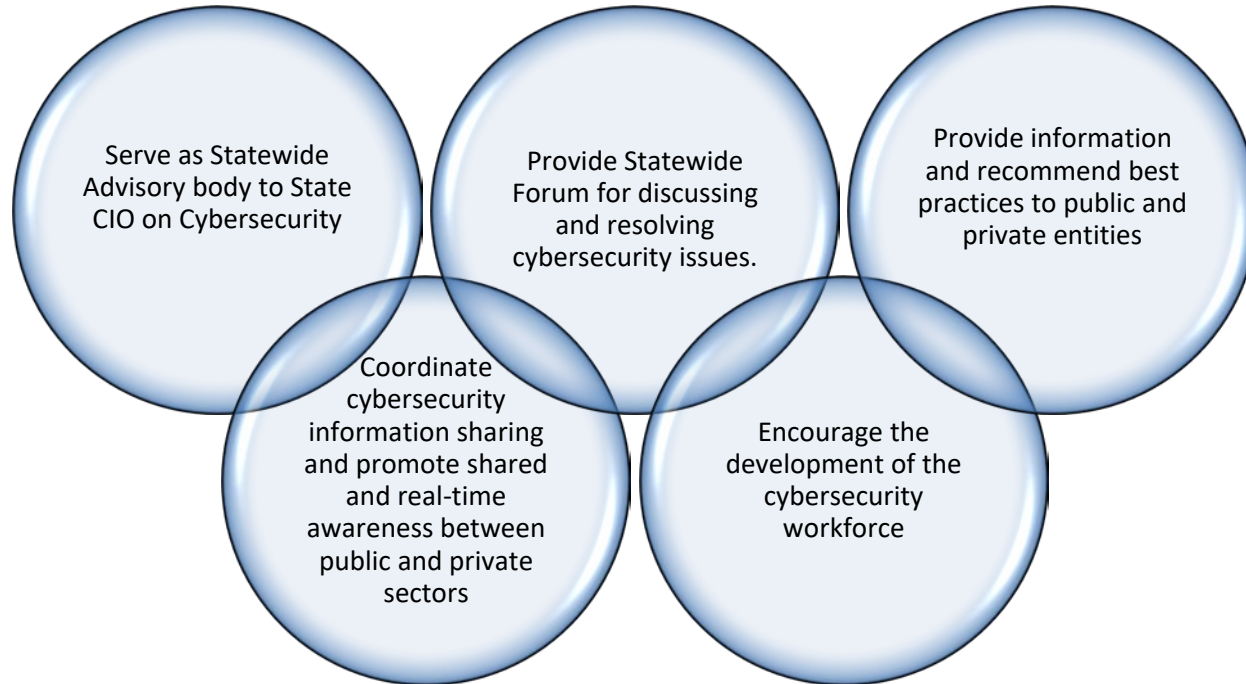
Cara Snow, Technology Association of Oregon

## Advisors

24 industry and educational experts



# Oregon Cybersecurity Advisory Council



# Public Cybersecurity Interventions

classes of interventions



# Cyber Center of Excellence

---

- SECTION 4. Oregon Cybersecurity Center of Excellence.
- The State Chief Information Officer shall develop a plan for the establishment of an Oregon Cybersecurity Center of Excellence. The State Chief Information Officer shall submit the plan to an appropriate committee or interim committee of the Legislative Assembly no later than January 1, 2019.





# PSU Research Findings



# Online Survey of Oregon Organizations

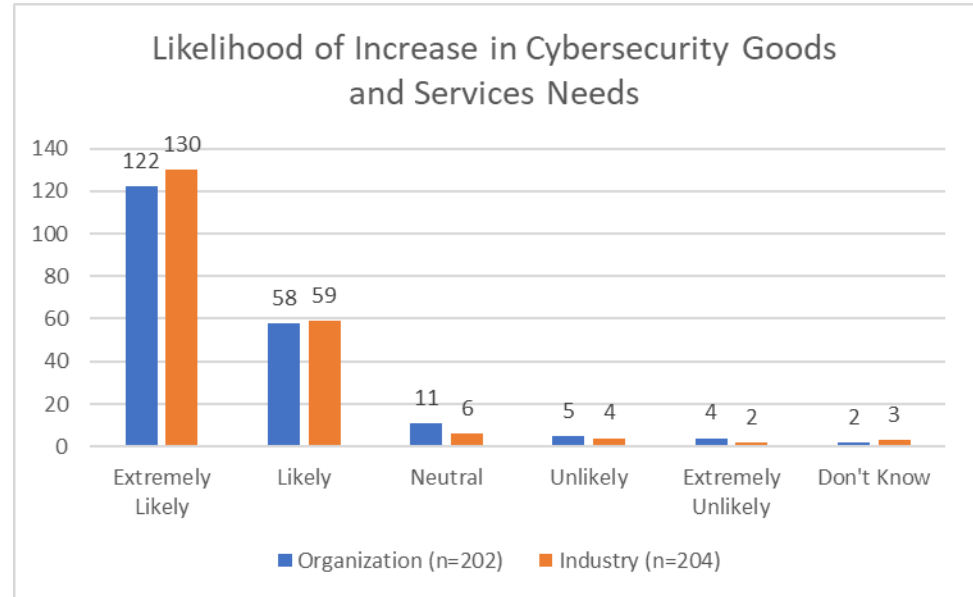
---

- The online survey of 205 respondents resulted in answers to 33 questions regarding the cybersecurity policies, practices, staffing, and concerns of Oregon organizations.



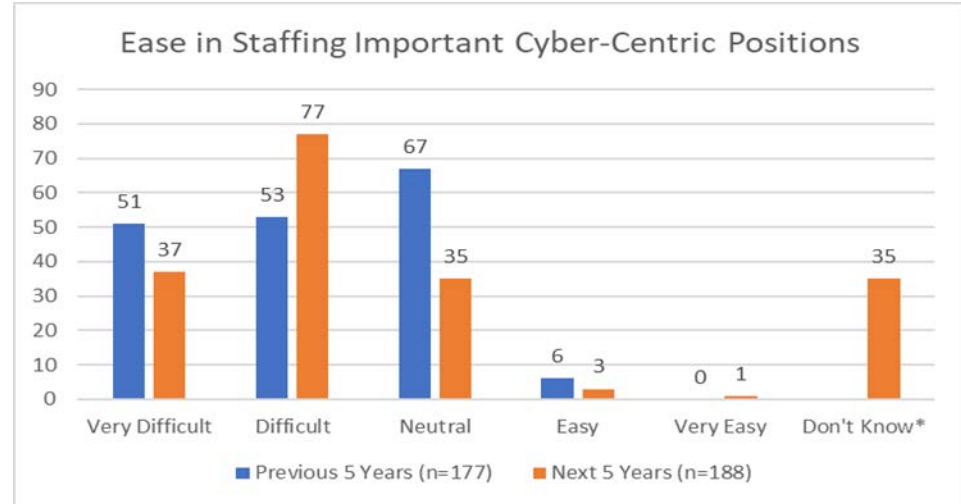
# Survey: Growing Needs

"...approximately 90% of respondents indicating that both their organizations and industries were likely or very likely to experience increased cybersecurity needs."



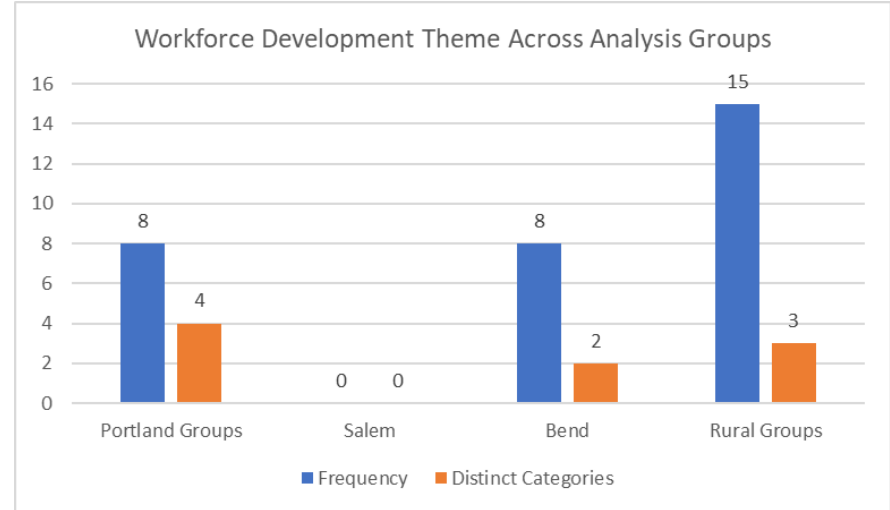
# Survey: Difficulty in Staffing

“Respondents do not find cybersecurity staffing to be an easy task, with approximately 59% reporting that staffing these positions has either been difficult (53 of 177, or 30%) or very difficult (51 of 177, or 29%) over the past five years”



# Focus Groups: Workforce Development

- **“Workforce development** as a theme featured pervasively in most conversations regarding potential CCoE activities and programs. Surprisingly, much of the conversation around workforce development focused on the **importance of K-12** education programs and other methods to introduce school-aged children to the cybersecurity field.”



# Oregon Cybersecurity Awareness Program



# Goals and objectives

---

- Build awareness across the state and beyond about Oregon's cybersecurity business and educational programs, talent and companies
  - Promote workforce development and create awareness of career opportunities
- Raise visibility of CCoE and support legislative initiatives
- Provide critical information and tools to help Oregon businesses and organizations improve cybersecurity

Cybersecurity in Oregon is not getting the visibility it needs.  
This program is designed to change that.



- One website/portal for all things Oregon cybersecurity
- Serves as a cybersecurity information clearinghouse
- Cross linked to sponsors and stakeholders
- Curated global cyber news
- Education achievements
- Contributed blogs
- Oregon cyber news
- Resource lists
- Research reports
- Success stories
- Webinars, events





# Oregon Cyber Summits

---

- 2018 Apr 23rd - University of Oregon Cybersecurity Day, Eugene
  - <http://securityday.cs.uoregon.edu/>
- 2018 June 20-22 – Global Cities Tech Jam, Portland
  - <http://www.techoregon.org/events/global-city-teams-challenge-tech-jam>
- 2018 July 19 - NW Cyber Camp with Cyber Summit – Mentor Graphics in Wilsonville.
  - [www.nwcyber.camp](http://www.nwcyber.camp)
- 2018 November 2 – Cybersecurity Education Summit – Bend, OR



## OUR SPONSORS

### PLATINUM



### GOLD



### SILVER



# Cybersecurity Center of Excellence

*Establishment Plan Summary*

[Available: https://bit.ly/2ICfXvU](https://bit.ly/2ICfXvU)



# CCoE Establishment Plan - Contents

This CCoE Establishment Plan addresses the required four types of primary activities and tasks specified in ORS 276A.326-29. The CCoE programmatic initiatives are envisioned as the following:

- Workforce development
- Education
- Extensive public outreach and awareness campaigns
- Public-facing incident response and recovery capabilities, in two key areas:
  - Creation of a threat information sharing and analysis (ISAO) node to participate in cybersecurity initiatives at the state and national levels– and serve as a liaison with the National Cybersecurity and Communications Integration Center within the United States Department of Homeland Security.
  - Completion and implementation of the Oregon Cybersecurity Strategy and Cyber Disruption Response Plans



# CCoE Establishment Plan - Status

---

- This CCoE plan is not currently funded, thus the development of the “center” as an entity is on hold
- The programs concepts proposed in the plan, were intended to serve as a guideline and exemplars for the types of programs that could be grown/accelerated under the center
- OCAC is completely flexible in the structure, phasing, and implementation details around any subset of the plan that makes sense, and is able to secure appropriate funding



# CCoE Establishment Plan - Contributors

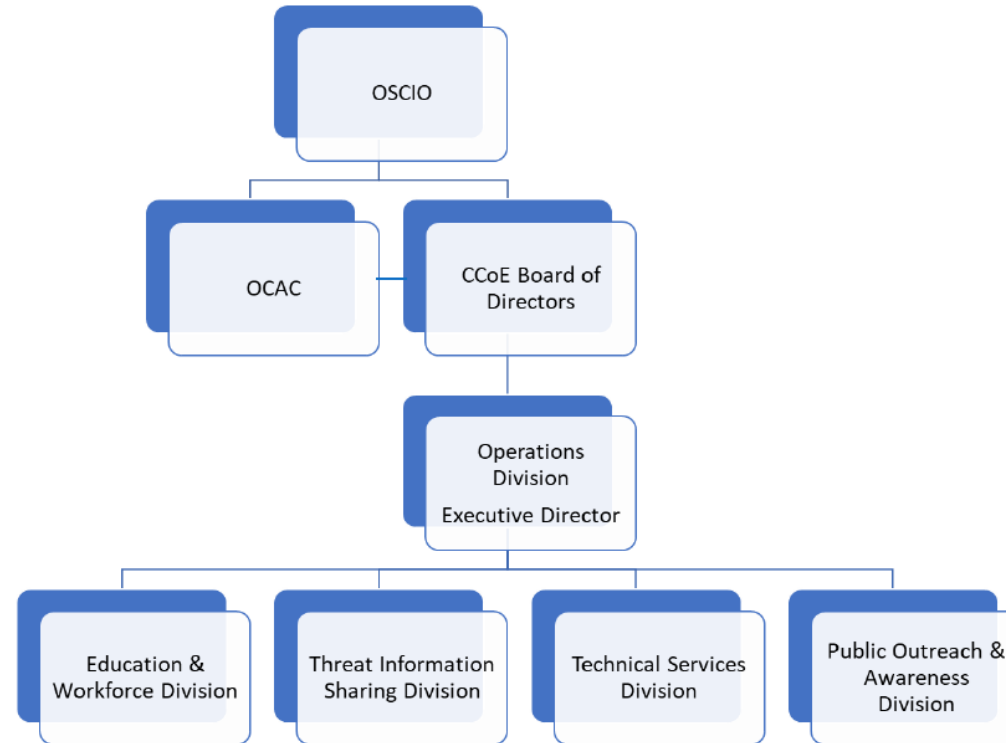
Name	Organization
Aaron Farraiuolo	UpTime Sciences
Abbar Ahmed	Cozera
Adam Rosenbaum	
Adam Silberman	Learning.com
Alyssa Macy	Warm Springs Tribe
Andrew Zambrano	EnergySec
Anickor, Kevin	Mosaic 451
Barber, David	OSU
Bob Cummings	LFO
Bob Kraus	ID Mentor
Bob Miller	OSU
Bonnie Petersen	Confederated Tribes of Siletz Indians
Brian Page	OregonTech CDC
Candace Worley	McAfee
Carla Axtman	Oregon Dept. of Administrative Services
Charles Wright	Portland State University
Christopher Rhen	Lane Community College
Dan C. Martin	McAfee
Dan Eyring	Cayuse
Dan Gullick	Aruba /HPE
Dan Manson	Cal Poly Pomona
Dave Nevin	OSU
Dean Adams	Burns / Piute Tribe
Delores Pigsley	Confederated Tribes of Siletz Indians
Deron McElroy	Oregon State
Dianne Greenlee	Oregon Dept. of Justice
Doug Kinoshita	Secure Works
Douglas Olson	Juniper Networks
Elizabeth Schaedler	RSA
Ellie Harmon	Portland State University
Emily Smith	Dalton Advocacy
Eric Hawley	Burns / Piute Tribe
Eric Quaempts	Cayuse - Umatilla - Walla Walla Tribes
Gary Mortensen	
Glencora Borradaile	School of EECS, Oregon State University

Greg Hughes	FISERV
Hammad Kahn	Revcastor
Isaac Potoczny-Jones	Tozny
Jack Estep	RSA
Jared Swezey	UpTime Sciences
Jason Adsit	Oregon National Guard
Jeff McClunkin	Teaches NSA & Cybersecurity
Jeff Williams	The Standard
Jenks, Michael	Mosaic 451
Jennifer Cecil	HPE Security
Jessica Odum	Lewis & Clark CTO
Johan DuPuis-Lund	Aruba /HPE
Johnathan Mocan	Burns / Piute Tribe
Jon Hannis	BSIDES
Joseph FitzPatrick	BSIDES
Julie Bettles	Klamath Tribe
Kedma Ough	Mt. Hood Comm College, SBDC
Kelly McElroy	Oregon State University Libraries
Kris Rosenberg	OIT
Laura McKinney	Oregon Tech
Lee Crum	Aruba /HPE
Lee Howell, MBA, CISSO, CISA	University of Oregon
Leo Howell	University of Oregon
Leslie Golden	Instil Security
Lisa Griffith	Thomson Reuters
Logan Kleier	Amazon Web Services
Mario Tarin	Secureworks
Marisol Revis	Xerox
Mark Cooper	PKI Solutions
Mark Ghazai	Microsoft
Melody Riley-Ralphs	OregonFiber
Michael Clark	Newberg Police
Nai Saechin	Sword & Shield
Nathanael Coffing	Cloudentity
Nic Endicott	Cayuse
Nicholas C. Harris	Oregon State Police
Nirupama Bulusu	Portland State University
Paul Maunder	Palo Alto Networks
Priscilla Oppenheimer	Southern Oregon University
Promod Antony	JBC Software
Rick Kam	

Roberta Frost	Klamath Tribe
Ronald Waters	Homeland Security
Ruth Swain	Oregon SBDC
Sean Torassa	Symantec
Shannon Marheine	Oregon DOJ
Steve Corbato	OregonFiber
Steve Parker President, EnergySec	Energy Sec
Steven Corbato, Ph.D	Oregon Fiber Partnership
Stuart McKee	Microsoft
Terry Braught	Center for Advanced Learning
Tobin Shields	MHCC
Topher Timzen	BSIDES
Twila Denham	EnergySec
Vasa, Lisa	Oregon State
Veronica Hotton	Portland State University
Vince Jacques	
Wayne Machuca	MHCC
Wu-chang Feng	Portland State University
Zach Swick	Oregon Emergency Management/Oregon Military
Zander Work	OSU



# Proposed CCoE Organization



# CCoE Potential Partners

Proposed CCoE Partnerships	CCoE Divisions				
	Operations	Education & Workforce Development	Threat Information Sharing	Technical Services	Public Awareness & Engagement
<b>Educational Institutions</b> <ul style="list-style-type: none"> <li>• K-12</li> <li>• Higher Educational Institutions</li> </ul> <b>Educational Initiatives</b> <ul style="list-style-type: none"> <li>• NW Cyber Camp</li> <li>• OSU OR Security Operations Center (SOC)</li> <li>• Oregon Fiber Partnership</li> <li>• MHCC Center for Academic Excellence Cybersecurity &amp; Networking Program</li> </ul>	Companion Resource	Operational Partner	Companion Resource	Operational Partner	Companion Resource
<b>Workforce Development</b> <ul style="list-style-type: none"> <li>• OSU OR Security Operations Center (SOC)</li> <li>• Oregon Pathways Project</li> <li>• Oregon Veterans Cybersecurity Initiative</li> </ul>	Companion Resource	Operational Partner		Operational Partner	Companion Resource
<b>Private Industry</b> <ul style="list-style-type: none"> <li>• IT</li> <li>• Cybersecurity</li> <li>• Small business entities</li> <li>• Business associations</li> <li>• Chambers of Commerce</li> <li>• BSIDES</li> </ul>	Companion Resource	Companion Resource	Companion Resource	Operational Partner	Companion Resource





# CCoE Potential Partners

Proposed CCoE Partnerships	CCoE Divisions				
	Operations	Education & Workforce Development	Threat Information Sharing	Technical Services	Public Awareness & Engagement
<b>Entities Engaged in Cybersecurity</b> <ul style="list-style-type: none"> <li>• OR State DAS / OSCIO</li> <li>• Oregon National Guard</li> <li>• FBI</li> <li>• Dept of Justice</li> <li>• OR State Police</li> <li>• Oregon Titan Fusion Center</li> <li>• Dept of Homeland Security</li> <li>• Multi-State Information Sharing and Analysis Center (MS-ISAC)</li> <li>• Regional and Sector-specific ISAOs</li> <li>• Adjacent states</li> <li>• FBI</li> <li>• DOJ</li> <li>• ISAO.org (UT at San Antonio)</li> </ul>	Companion Resource	Companion Resource	Companion Resource	Companion Resource	Companion Resource
<b>Public Agencies</b> <ul style="list-style-type: none"> <li>• State, local, and tribal entities</li> <li>• Special districts &amp; associations</li> <li>• County extension offices</li> </ul>	Companion Resource	Companion Resource	Companion Resource	Companion Resource	Companion Resource



# CCoE Program Concept #1

---

Project Name: NW Cyber Camp Expansion

Author(s): Charlie Kawasaki, CTO, PacStar

Overview: Currently, NW Cyber Camp is volunteer run and has been held at 5 locations (Portland, Gresham, Wilsonville, Bend, and Corvallis). It is a camp for high school students, introducing them to cyber security and creating a pipeline for the cyber security industry where there is a significant need for trained cyber security professionals. This proposal would require funding to expand to additional locations throughout the state, hire a paid program manager, and provide stipends for low-income students to assist them in participating in the camp.



# CCoE Program Concept #2

---

Project Name: Oregon Cyber Pathways Project

Author(s): Steve Parker, President, EnergySec

Twila Denham, Managing Director, Operations and Workforce  
Development, EnergySec

Overview: The Oregon Cyber Pathways Project (OCP) will seek out, identify, and guide future security professionals along their development path from youth-focused programs through internships and apprenticeships that establish them in the workforce. The OCP will work with school districts, youth organizations, academia, and businesses throughout Oregon to build and leverage a network of contacts to connect youth and young adults to organizations that provide cyber security education, competitions, mentoring, work experience, and long term careers in the field.



# CCoE Program Concept #3

---

Project Name: Managed Security Service Provider

Author(s): Charlie Kawasaki, CTO, PacStar and Vice-Chair of OCAC

Overview: Developed by the Technical Services Working Group of OCAC, this concept addresses the need for cyber security protections in place by large numbers of organizations (such as K-12 districts, small businesses, and non-profits) throughout the state that are unattractive for commercial cyber security companies due to their lack of funding, remote locations, or lack of capacity.

***The MSSP includes the Oregon Institute of Technology concept of an extension service model, which deploys university students and faculty to assist with cybersecurity needs.***



# CCoE Program Concept #4

---

Project Name: Oregon Veteran Cybersecurity Initiative (OVCSI)

Author(s): Rick Kam, Bob Kraus, Vince Jacques, Adam Rosenbaum, Gary Mortensen

Overview: Engage veterans to work directly with other veterans to identify where they can apply their interests and service experience with the goal of connecting them with institutions in Oregon that are hiring cybersecurity professionals. Would require funding for programming, staff, and website development.



# CCoE Program Concept #5

---

Project Name: Cyber Oregon Public Outreach/Awareness

Author(s): Skip Newberry, President & CEO, Technology Association of Oregon

Tom Quilin, CTO Security Economics, McAfee

Megan McKenzie, CEO, McKenzie Worldwide

Overview: The concept seeks to build awareness across the state and beyond about Oregon's cybersecurity business and education programs, talent, and companies; promote workforce development and create awareness of career opportunities; raise visibility of cybersecurity and support legislative initiatives; and provide critical information and tools to help Oregon businesses and organizations improve cybersecurity. Funding for maintaining a website and supporting staff in managing content, advertising, etc. would be required.



# CCoE Program Concept #6

---

Project Name: Oregon State University's Oregon Research & Teaching Security Operations Center (ORTSOC)

Author(s): Rakesh Bobba, Dave Nevin, David Barber

Overview: Partner with Oregon State University to build the ORTSOC into a world-class teaching and research Security Operations Center that offers learning opportunities for undergraduate students, offers cybersecurity training and education opportunities for IT staff of small businesses, creates opportunities for researchers at OSU and partners to develop new approaches in cybersecurity protection, help address operational security needs at Oregon institutions of higher education, and provide cybersecurity information sharing and potentially threat assessment and monitoring services as well for the Oregon Cybersecurity Center of Excellence. This proposal would be supported by funding to expand existing services, staff and student positions, as well as a small amount for equipment.



# CCoE Program Concept #7

---

Project Name: Security and Privacy Education for the General Public through Libraries

Author(s): Kelly McElroy, OSU Libraries

Glencora Borradaile, School of EECS, OSU

Overview: A training program for librarians across Oregon to build skills and capacity for general education in computer security and privacy. The training program will consist of 3-6 month weekly distance-learning activities including lectures, readings, and hands-on activities, along with two days of intensive in-person training. This proposal would support 3 cohorts of 20-30 librarians.

Funding would be needed to administer the program, pay for staff time to develop materials, recruit participants, and evaluate the program.





# CCoE Program Concept #8

---

Project Name: Broadening Security Education in Oregon

Author(s): Wu-change Feng, Ellie Harmon, Charles Wright, Nirupama Bulusu, and Veronica Hotton, Portland State University

Overview: This concept would be to expand current cybersecurity education efforts for technical and non-technical audiences. The non-technical trainings would expand existing CyberPDX programs, security awareness, and phishing curriculum. The concept would also increase training for technical audiences, including Saturday Academy ASE internships, Oregon CTF, and among other things, technical training that targets an emerging, underserved area in cloud and block-chain security. Funding would be required for curriculum development, mentorship, and event organization.



# CCoE Program Concept #9

---

Project Name: Business Education Concept Cyber Internship Model

Author(s): Tobin Shields and Terry Braught, Mount Hood Community College and Center for Advanced Learning

Overview: This concept proposes a unique internship model that focuses on short term, project-based, and high-need experiences that are facilitated by the Business Education Compact (BEC) and classroom instructors. The concept involves placing interns in organizations to work on cybersecurity related projects. Businesses would contribute funding to intern salary. Additional core funding would allow more businesses, students, and instructors to benefit from this experience.



# CCoE Program Concept #10

---

Project Name: Professional Certification Fund

Author(s): Tobin Shields, Mount Hood Community College

Overview: This proposal outlines the creation of a “certification scholarship fund” that allows students pursuing cyber education programs to apply for access to free or substantially reduced exam vouchers for industry certification exams offered through organizations like CompTIA, CISCO, and others. The program concept incorporates standards for eligibility and processes for allocating funding. This program would increase the Appendix A, p. 3 cybersecurity professionals and reduce barriers for entry into the workforce. This program is expandable based on the number of students and institutions involved in the effort.



# CCoE Program Concept #11

Project Name: BSIDES Portland

Author(s): Joseph FitzPatrick, Topher Timzen, Jon Hannis

Overview: BSIDES Portland is a 501(c)(3) organization that hosts the only annual information security-focused conference in Oregon. This concept proposal would allow BSides Portland to grow from the established volunteer-run information security / cybersecurity event it has been for the last 8 years into the professional information security/cybersecurity event that Oregon deserves. This proposal would support the Oregon information security community, allowing the community in turn to support the security needs of all citizens of Oregon. Funding for BSIDES would help support presenters' costs, allow for a greater number of highly impactful talks and workshops, support capture the flag competitions to more venues in Oregon, and will enable the documentation and publication of the event for the benefit of all Oregonians.



# Proposed CCoE Budgetary Estimate

CCoE Divisions	Estimated FTE Maximum for all Phases. Includes intern or student funding	Phase 1	Phase 2	Phase 3	All Phases
		Statewide Strategic Planning & Fundraising 10/1/2019 – 6/30/2020	Estimated Program Implementation July 2020 - June 2021	Estimated Program Implementation July 2021 - June 2022	
Operations Division	1.5	\$760,000.00	\$905,000.00	TBD	\$1,665,000.00
Education & Workforce Development Division	17.88		\$1,453,489.00	\$1,669,134.00	\$3,122,623.00
Threat Information Sharing Division	0.75		\$195,000.00	\$140,000.00	\$335,000.00
Technical Services Division	16.31		\$1,475,100.00	\$3,103,680.00	\$4,578,780.00
Public Outreach & Awareness Division	Contracted		\$653,970.00	\$641,260.00	\$1,295,230.00
<b>TOTAL</b>		\$760,000.00	\$4,682,559.00	\$5,554,074.00	\$10,996,633.00

- 85% of budget allocated directly to programs\*
  - 15% for operations also includes budget for statewide disruption plan
- 73% of budget allocated to workforce development, educational programs
  - Includes side benefit of increased, deployed cyber
- 12% for outreach and awareness



# Proposed CCoE Timeline

	Phase I: October 2019-June 2020				Phase II: July 2020-June 2021		Phase III: July 2021 +
	Q1	Q2	Q3	Q4	H1	H2	Y3
Cybersecurity Disruption and Strategic Plan (required biennially)	Scope plan requirements & identify resources	Identify plan implementation (contractors / staff)  Begin planning process with state-wide stakeholder engagement	Continue planning process & engage state-wide stakeholders	Complete plan	Implement plan		Evaluate plan and update for biennial submission
Resource Development & Strategic Planning	Analyze funding resources and collaborative partners for program implementation	Commence grant writing and other funding source activities	Coordinate and/or oversee program implementation as funding is available				
	Seek additional supporting resources						
Division Area Programmatic Plans	Assess funding availability and program planning	Engage partners in collaborative actions	Implement programs as partnerships and funding is available				
	Plan evaluation activities to demonstrate public benefit		Monitor programs and collect evaluation data		Evaluate program outcomes*		



# 2019 – 2020 Priorities and Activities



# 2019 OSCIO & OCAC Joint Priorities

---

- OCAC technical advisory work group. The OCAC technical working group could serve as a technical advisory function to the state CISO, helping them vet plans and policies.
- Internship program(s). The State has a significant cybersecurity workload in a competitive market for cybersecurity talent. OCAC can collaborate to develop workforce and internship programs.
- OCAC collaboration on one or more cybersecurity services and technologies that OSCIO provides to the State – addressing scalability and sustainability items.





# Testimony

## Christopher Reekie

### Student, Oregon Episcopal School



# Christopher Reekie - Testimony

---

- Was able to attend NW Cyber Camp and make connections within the cybersecurity industry
- Has internship as a result of prior connections rather than an established internship program
- Increased funding for cybersecurity related programs in and out of schools would improve knowledge surrounding systems security



# Testimony

## Zander Work

### Student, Oregon State University



# My Background

---

- Went to Lake Oswego HS
  - There weren't any CS classes
  - Had to find other opportunities to fuel my passions
- Interned at Portland State
  - Saturday Academy's Apprenticeships in Science & Engineering (ASE)
- Met Charlie, interned at PacStar
  - Informal (no established internship program)

## Current:

- Sophomore at Oregon State University (Security option)
- Student Analyst in the Oregon Research & Teaching Security Operations Center (ORTSOC)
- President of the OSU Security Club (<https://www.osusec.org/>)

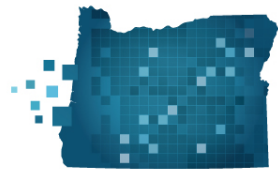


# Importance of Security Education

- Current offerings are lacking
  - Few/no formal internship programs
  - Few/no curriculum in high schools
- This leads to minimal exposure to the field
  - Students don't get excited about it because they don't know it exists
- Programs like the NW Cyber Camp help with this, but more needs to be done
  - Formal internship programs
  - HS courses

**Invest in students, you'll have a guaranteed return (I'm proof of that)**





**CYBEROREGON**

---

Questions?

