



Oregon Cybersecurity Center of Excellence

Creating a Central Cybersecurity Resource
Hub for All Oregonians

Establishment Plan



OREGON | Office of the State

Chief Information Officer

Oregon Cybersecurity Center of Excellence Establishment Plan

Oregon Cybersecurity Advisory Council

Kerri Fry – *Chair*, IGNW
Charlie Kawasaki, CISSP - *Vice Chair*, PacStar
Megan McKenzie - *Secretary* (non-voting), McKenzie Worldwide
Rakesh Bobba, Ph.D, Oregon State University
Michael Gutsche, Micro Focus International
Ken Kestner, Lake County
Skip Newberry (*non-voting*), Technology Association of Oregon
Andrew Plato, Anitian
Tom Quillin, McAfee LLC
Dennis Tomlin, CISSP, HCISPP, ITIL, Multnomah County
Mike Wells, Oregon Department of Justice
Office of the State Chief Information Officer Appointee



Drafting and Research Assistance

Center for Public Service
Mark O. Hatfield School of Government
Portland State University

Margaret E. Banyan, Ph.D – *Project Manager*
Marcus Ingle, Ph.D – *Faculty*
Kent Robinson, Ph.D - *Faculty*
Jess Daly, MPP – *Policy Analyst*
Isaac Butman – *Graduate Research Assistant*
Emily Vilorio – *Graduate Research Assistant*



TABLE OF CONTENTS

Table of Contents	3
Executive Summary	6
Definitions and Acronyms.....	7
Section 1- Introduction.....	8
1.1 OVERVIEW OF THE ESTABLISHMENT PLAN	8
Section 2 - Background.....	9
2.1 OREGON CCoE MISSION AND FRAMEWORK FOR ACTION	9
2.1.1 Mission and Rationale	9
2.1.2 Framework for Action.....	11
Section 3 – Research and Planning Basis of CCoE Plan.....	13
3.1 CCoE AND OCAC RESPONSIBILITIES: OREGON LAW ORS276A.326-29	13
3.1.1 CCoE Responsibilities.....	13
3.1.2 OCAC Responsibilities	13
3.2 EVIDENCE-BASED RESEARCH.....	13
3.2.1 Survey Results	14
3.2.2 Focus Groups.....	14
3.3 OREGON CYBERSECURITY ADVISORY COUNCIL ROLE AND SUPPORT.....	15
3.3.1 CCoE Statutory Task Breakdown by Assigned CCoE Divisions	15
Section 4 – CCoE Governance Structure	18
4.1 PROPOSED GOVERNANCE STRUCTURE	18
4.2 PROPOSED CCoE ORGANIZATIONAL STRUCTURE	18
Section 5 - CCoE Division Area Programmatic plans.....	19
5.1 OPERATIONS DIVISION	19
5.1.1 Operations Division Overview.....	19
5.1.2 Operations Division Tasks and Alignment with SB90.....	19
5.2 EDUCATION AND WORKFORCE DEVELOPMENT DIVISION	21
5.2.1 Education and Workforce Development Division Overview	21

5.2.2 Education and Workforce Development Tasks and Alignment with SB 90.....	22
5.2.3 Possible Operational Partners & Companion Resources	23
5.3 THREAT INFORMATION SHARING DIVISION	24
5.3.1 Threat Information Sharing Division Overview	24
5.3.2 Threat Information Sharing Tasks and Alignment with SB90	24
5.3.3 Possible Operational Partners and Companion Resources	26
5.4 TECHNICAL SERVICES DIVISION	27
5.4.1 Technical Services Division Overview	27
5.4.2 Technical Services DIVISION Tasks and Alignment with SB90	27
5.4.3 Possible Operational Partners & Companion Resources	29
5.5 PUBLIC OUTREACH AND AWARENESS DIVISION.....	30
5.5.1 Public Outreach and Awareness Division Overview	30
5.5.2 Public Outreach and Awareness Tasks and Alignment with SB90	30
5.5.3 Possible Operational Partners & Companion Resources	31
Section 6 - Timeline Overviews & Implementation Phasing	32
Section 7 - Budget, Financial Resources, and Potential Partners	33
7.1 BUDGET NARRATIVE	33
7.2 BUDGET	34
7.3 FUNDING STRATEGY	35
7.3.1 Grant Opportunities	35
7.3.2 Federal Funding.....	35
7.3.3 Foundation and Private Sources.....	36
7.3.4 Membership or Service Fees.....	36
7.3.5 Other Funding Vehicles.....	36
7.3.6 Funding Strategy Summary.....	36
7.4 PARTNERSHIPS & SHARED RESOURCES	37
7.4.1 Proposed Operational Partners & Companion Resources	37

7.4.2 Committed Resources.....	38
Section 8 - Public Value Measurement and Evaluation	39
Acknowledgements	40
End Notes.....	43
Appendices.....	45

EXECUTIVE SUMMARY

The cost and number of cyber crimes in Oregon is increasing. For example, the number of FBI documented cyber related complaints in Oregon rose from 961 in 2014 to 3,455 in 2017, with the cost to Oregonians increased from \$2.9 million in 2006 to \$11.1 million in 2017. Just in the last decade, the total documented cost to Oregonians, was a staggering \$74 million dollars. The FBI data only includes reported losses. Including the loss of time, costs of recovery, and response, estimates place this number closer to \$1.6 billion annually.¹

To respond to this challenge, Oregon's Senate Bill 90 (ORS 276A.326-9), signed into law and effective as of July 1, 2017, requires the Oregon Office of the State Chief Information Officer (OSCIO) to draft an Establishment Plan for the Oregon Cybersecurity Center of Excellence (CCoE).

This Plan integrates previous and current research conducted by the Center for Public Service at Portland State University (CPS),² Oregon Cybersecurity Advisory Council working group contributions, and guiding documents from the Oregon State Chief Information Officer.^{3,4} The Plan is informed and framed by 18 months of intensive academic research, robust public engagement of many individuals and businesses, expert information technology (IT) security advising from the Oregon Cybersecurity Advisory Council (OCAC), and an assessment of stakeholder and beneficiary needs.

This document outlines the CCoE establishment plan. It proposes a governing structure that features a Board of Directors that will oversee an Executive Director and five Divisions (Operations, Education and Workforce Development, Threat Information Sharing, Technical Services, and Public Outreach and Awareness).

The CCoE proposes to develop in phases. The first phase would begin in October 2019 and would be dedicated to establishing the Center and implementing statutorily required planning. The following phases are intended to implement Divisions and their programs as funding becomes available.

The budget to fund the required statewide planning efforts would be \$1,665,000 over two fiscal years. To fully fund the programmatic plans, would require an additional \$9,331,633. However, programs and priorities may change, or overlap, based on the findings of the statewide strategic plans and/or funding availability. Additionally, Division budgets may be scaled up or down, depending on the phasing strategy and funding availability. The CCoE is aware that the legislative appropriations process involves a certain element of uncertainty and this effort must be prepared with funding contingency plans.

Finally, this Plan outlines the significant public benefit of the CCoE. Its role as an economic and workforce development engine, coupled with the significant cost savings, has enormous potential for all Oregonians.

DEFINITIONS AND ACRONYMS

Active Monitoring	Active monitoring, or continuous monitoring, is a cybersecurity risk management strategy that provides for near real time security status and early detection of threats ⁵
CCoE	Cybersecurity Center of Excellence
CDC	Center for Disease Control
CIO	Chief Information Officer
CPS	Center for Public Service, Hatfield School of Government, Portland State University
Cyber hygiene	Cyber hygiene refers to routine and/or preventative measures that are designed to avoid attack and limit the spread of infection. An example of cyber hygiene is safe browsing habits where dangerous phishing attacks, email attachments, and nefarious sites are avoided
Cyber immunization	Cyber immunization is a result of good cyber hygiene where systems are protected against attack through preventative measures, such as software updates
Coordinated incident response	Coordinated incident response is defined as a rapid containment of cybersecurity outbreaks
ED	Executive Director
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
LC	Legislative Concept
MSSP	Managed Security Services Provider
OCAC	Oregon Cybersecurity Advisory Council
ORTSOC	Oregon Research and Teaching Security Operations Center
OSCIO	Office of the State of the Chief Information Officer
SOC	A security operations center (SOC) generally describes a team that is dedicated to preventing, detecting, assessing, and responding to cyber attacks or threats

SECTION 1- INTRODUCTION

1.1 OVERVIEW OF THE ESTABLISHMENT PLAN

Oregon's Senate Bill 90 (ORS 276A.326-9), signed into law and effective as of July 1, 2017, requires the Oregon Office of the State Chief Information Officer (OSCIO) to draft an Establishment Plan for the Oregon Cybersecurity Center of Excellence. The Plan presented in this document was collaboratively prepared by the Oregon Cybersecurity Advisory Council, OSCIO, and the Center for Public Service at Portland State University (CPS). This document integrates previous and current research conducted by the Center for Public Service at Portland State University (CPS),⁶ Oregon Cybersecurity Advisory Council working group contributions, and guiding documents from the Oregon State Chief Information Officer.^{7,8} This Plan is informed and framed by 18 months of intensive academic research, robust public engagement, expert information technology (IT) security advising from the Oregon Cybersecurity Advisory Council (OCAC), and an assessment of stakeholder and beneficiary needs. The intensely collaborative process has culminated in the following Oregon Cybersecurity Center of Excellence Establishment Plan document.

The Plan is organized around in the following major sections:

- Section 1- Introduction
- Section 2- Background
- Section 3- Statutory Requirements
- Section 4- CCoE Governance and Structure
- Section 5- CCoE Division Area Programmatic Plans
- Section 6- Timeline Overviews - Implementation Phasing
- Section 7- Comprehensive Budget and Financial Resources Roll Up
- Section 8- Public Benefit and Value Measurement and Evaluation

SECTION 2 - BACKGROUND

2.1 OREGON CCOE MISSION AND FRAMEWORK FOR ACTION

2.1.1 MISSION AND RATIONALE

The Oregon Cybersecurity Center of Excellence (CCoE) was tasked by ORS 276A.329 to serve as a central civilian resource hub for coordinating a broad variety of public cybersecurity needs that are strategic, educational, and remedial. The CCoE features multi-sector engagement with a diverse geographical reach. In addition, the CCoE is responsible for developing two statewide strategic planning initiatives.

The CCoE plans to deliver significant public benefit and shared value aimed at protecting Oregon's interconnected systems against growing and costly threats. Multiple studies have shown that the incidence and number of cyber crimes are rising. Consider, for example the following national statistics:

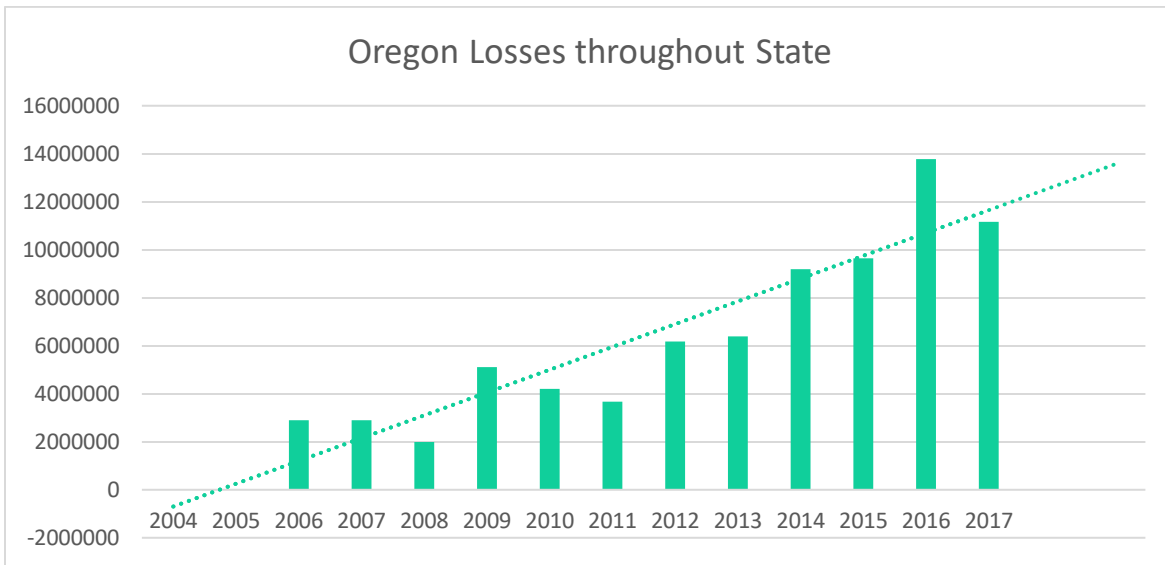
- Losses in 2017 alone: \$1.4 Billion⁹
- The average cost of a breach to a small business is between \$84,000 and \$148,000.¹⁰
- Time to recover from a breach approximately 50 days
- 43% of breaches affect small companies
- 60% of small businesses close within six months following a breach¹¹

In Oregon, the cost and number of cyber crimes is more dramatic. Based on the FBI's Internet Crime Complaint Center and other studies, Oregonians are at risk based on the following:¹²

- Number of Complaints in Oregon rose from 961 in 2014 to 3,455 in 2017
- Table 1 below shows that the cost to Oregonians rose from \$2.9 million in 2006 to \$11.1 million in 2017.
- The total reported cost to Oregonians in the last decade (2007 to 2017) alone is a staggering \$74 million dollars

However, not all breaches are reported. This could be for reasons ranging from a breach not meeting the threshold for reporting or for a business failing to report. Just for small businesses, the cost of a breach is much larger than the FBI data shows. In 2015 there were 89,469 small businesses that employed between 1-499 people. If one applied the national statistic, estimating that 54% that will suffer a breach within one year, the cost to these businesses would be approximately \$1.6 billion annually.¹³

TABLE 1: OREGON LOSSES DUE TO CYBERCRIME



Responding to these losses requires a skilled workforce to prevent, respond, and mitigate cyber attacks. Oregon is behind in securing the professionals needed to respond, as there are currently more than 2,900 jobs in cybersecurity open.¹⁴ Oregon’s supply of cybersecurity professionals is considered to be very low.¹⁵

In order to respond to these risks and protect Oregonians, a coordinated effort is required. This effort must be multidisciplinary, geographically diverse, and involve the efforts of the private, public, and nonprofit sectors.

This CCoE Establishment Plan aims to fulfill that requirement. At the forefront of the CCoE is the value of education and workforce development as a core drivers of change. The goal of the CCoE is to secure and protect Oregon’s growing economy while providing hands-on teaching and learning in a way that leverages cybersecurity education and advancement opportunities in Oregon. To accomplish this, the CCoE will work collaboratively with partners across the state of Oregon, with a Board of Governors.

Throughout the Oregon CCoE Establishment Plan, significant attention has been paid to identifying opportunities for potential public benefit and value creation. The Oregon CCoE proposes a set of high value programs that have significant public benefit, especially with regard to educating and providing benefits to underserved populations across the state. Together, these proposed programs promise to significantly increase access to, and raise awareness of, cybersecurity information, educational opportunities, tools, and services across Oregon.

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:¹⁶

- 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

2.1.2 FRAMEWORK FOR ACTION

The Oregon Cybersecurity Center of Excellence (CCoE) was envisioned by the Oregon Legislature to be an integrated cybersecurity resource hub working to protect Oregonians. The underlying framework of the CCoE involved a shared responsibility for cybersecurity.¹⁷ It proposes to respond to the substantial evidence growing over the last decade that while network-wide cybersecurity is a public good, it is currently underdeveloped and underfunded.¹⁸

“While community institutions may fall outside the traditional ambit of state cyber security policy, our interdependence and shared information systems render individual and isolated interventions insufficient to stem the tide of cyber security threats. We are more resilient when we stand together.”

- Oregon Office of the State Chief Information Officer

Based on these challenges, the OSCIO supported a research framework that examines cybersecurity using a public health model from the Center for Disease Control (CDC), comparing existing cybersecurity initiatives in other states with those resembling the planned responsibilities and statutory vision for the Oregon CCoE.¹⁹ The evidence shows that the best approach is for individuals, organizations, and governments to all share a responsibility in keeping networks and computer systems secure.^{20,21,22}

This requires keeping these networks and systems free from infection, providing nimble and robust response, engaging in effective recovery, and astutely concentrating on strategy, prevention, and proper cyber hygiene.^{23,24}

In Phase I of its research, the Center for Public Service (CPS) identified innovative practices for comprehensive and interoperable cybersecurity emphasizing a four-part model, geared toward creating a central hub that could provide competent leadership to address three key areas: prevention, active monitoring, and response and recovery of cyber ecosystems^{25,26} These categories cover the range of required objectives set forth in the SB 90 legislation (a summary of which can be found on page 13 of this document). The four categories of Leadership, Prevention, Active Monitoring, and Response and Recovery comprise the framework used to align the CCoE’s Establishment Plan and overall mission with the required statutory tasks, as well as with the CPS Cybersecurity Needs Assessment findings. This framework is illustrated below in Figure 1: CCoE Implementation Framework.²⁷

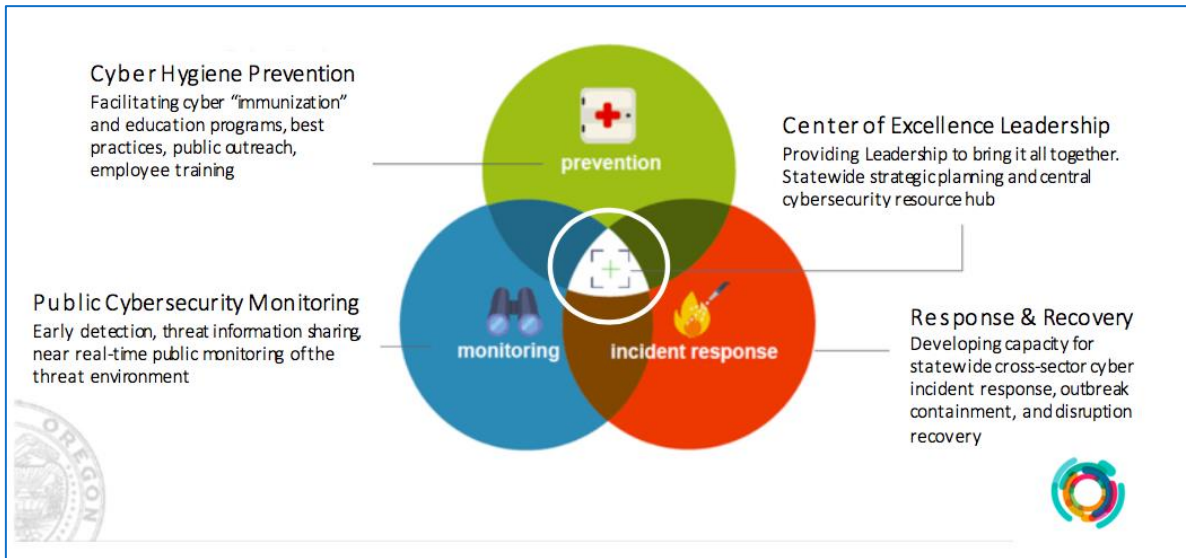


FIGURE 1: CCOE IMPLEMENTATION FRAMEWORK

SECTION 3 – RESEARCH AND PLANNING BASIS OF CCOE PLAN

3.1 CCOE AND OCAC RESPONSIBILITIES: OREGON LAW ORS276A.326-29

3.1.1 CCOE RESPONSIBILITIES

The OSCIO is required to submit the CCoE Establishment Plan to an appropriate committee or interim committee of the Legislative Assembly no later than January 1, 2019.²⁸ The Plan must include a description of the actions, timelines, budget, and positions or contractor resources required for the center to accomplish the tasks within ORS276A.326-29. The tasks are represented below.

- Coordinating information sharing regarding cybersecurity risks and incidents across all types of organizations.
- Drafting and biennially update, the State of Oregon Cybersecurity Strategy, and Oregon Cyber Disruption Response Plan.
- Supporting cybersecurity incident responses and investigations.
- Serving as an Information Sharing and Analysis Organization that officially liaises with the National Cybersecurity and Communications Integration Center.
- Participating in federal, multi-state, and private sector organizations that are relevant to the mission and activities of the CCoE.
- Receiving and disseminating cybersecurity threat information from a wide range of sources.

3.1.2 OCAC RESPONSIBILITIES

ORS 276A.326-29 also outlines the responsibilities of the OCAC. These OCAC responsibilities are as follows:

- Serve as the statewide advisory body to the State CIO on cybersecurity.
- Providing a statewide forum for discussing cybersecurity issues.
- Recommending best practices for cybersecurity to all types of organizations.
- Promoting cybersecurity real-time situational awareness for all types of organizations.
- Encouraging cybersecurity workforce development.

3.2 EVIDENCE-BASED RESEARCH

To assist with the process of drafting this Plan, OCAC and OSCIO engaged Portland State University's Center for Public Service (CPS) to conduct comprehensive research on the state of cybersecurity in Oregon and initiatives in other states that could serve as templates for the CCoE to follow. CPS conducted research activities, which were presented in an earlier report entitled, *A Cross-Sector Capabilities, Resources, and Needs Assessment: Research to Support the Drafting of the Oregon Cybersecurity Center of Excellence Proposal*. (Cybersecurity Needs Assessment)²⁹ The extensive 178-page report included:

- A policy analysis of cybersecurity efforts in other states examined through a public health lens, including an extensive review of strategic efforts and plans in those states;
- An online survey of Oregon organizations regarding their cybersecurity policies, processes, staffing, and needs;

- Cross-sector focus groups with cybersecurity professionals throughout Oregon;
- Catalogs of current funding opportunities for potential CCoE activities;
- An inventory of cybersecurity resources that currently exist in Oregon.

The following section provides a summary of the Phase I research findings. These findings guided the development of the CCoE Division’s programmatic plans. Additional research was conducted in a second phase that focused on further defining programmatic concepts as the mechanism by which the CCoE fulfills its responsibility to the state. The second phase also included support for drafting this Oregon CCoE Establishment Plan.

3.2.1 SURVEY RESULTS

As noted above, the CPS conducted survey research as a way to better understand the need for cybersecurity tools and programs. Of the 174 respondents,³⁰ the findings were as follows:

Need for Services: 90% of respondents recognized the need for attention to cybersecurity goods and services. These respondents indicated that their organizations and public agencies, industries, and other entities with whom they interacted were likely or very likely to experience increased cybersecurity needs.

Need for Cybersecurity Professionals: 75% of all respondents across all industries and organizations said that cyber expertise is either critical or very important to their typical operations. Despite this, approximately 59% of organizations reported that staffing has been difficult or very difficult over the past five years. In addition, 84% thought there would be a significant or moderate shortage of qualified workers for important positions.³¹

Need for Programs: When asked about cybersecurity resources or programs, there were many that respondents agreed they would use. 78% indicated they would use a state-wide cyber event warning system; 65% would use a fully online continuing education and certification program; 63% would attend cybersecurity information sharing events; and 63% would use low-cost reviews of cybersecurity systems.

3.2.2 FOCUS GROUPS

Additional research was conducted using eight (8) focus groups attended by a wide variety of industry professionals, including those from education, finance, government, healthcare, information technology, AMTUC (agriculture, mining, transportation, utilities, and construction), and other sectors. Several themes were apparent from this process, including the following:

Education and workforce development were high priorities and were seen as a means to attract businesses to graduates in Oregon and/or locating in the state. One participant noted, “If [the CCoE] can incentivize those people not to leave the state, business will come here to get that talent.” – Bend, Healthcare and Medical industry

Services needed throughout the state. In terms of service needs, the focus group findings showed that there was a significant interest in serving and including organizations that are smaller in size and geographically distributed throughout the state.

Trustworthiness. Finally, the focus groups found that the importance of trustworthiness and trust while sharing information and participating with a CCoE. Specifically, “participants in most analysis groups expressed a need for assurances of the trustworthiness of those with whom they’d be expected to share.” The widespread concern as to with whom information is shared underscores the expressed need for a neutral broker, such as a CCoE, that is a trusted partner in cybersecurity.

3.3 OREGON CYBERSECURITY ADVISORY COUNCIL ROLE AND SUPPORT

The responsibility to submit this Establishment Plan rests with the OSCIO. In order to accomplish its development, the OSCIO delegated the task of developing the Plan to OCAC. Based on the recommendations of the CPS Oregon Cybersecurity Needs Assessment, the OCAC created four working groups to divide the CCoE tasks including: Operations, Workforce & Education, Technical Services, Public Outreach & Awareness, and Information Threat Sharing. The workgroups brought together a range of experts to create initial programmatic concepts to fulfill the required CCoE functions, providing the source of this Plan’s budgetary estimates. A short summary of exemplary programs appears in Appendix A. In addition, the programmatic plans identified many possibilities for partnerships and programs. Additional detail describing these partnerships are included later in this Plan as part of the programmatic offerings of the CCoE.

3.3.1 CCOE STATUTORY TASK BREAKDOWN BY ASSIGNED CCOE DIVISIONS

The CCoE program actions consist of four categories of cybersecurity activities. These areas are Leadership (Operations), Prevention, Monitoring, and Response & Recovery. Each category includes several sub-categories of activities that are recognized by the literature as essential to a cross-sectoral and state-wide cyber readiness plan to maintain healthy cyber ecosystems. Figure 2, below illustrates the activities and their components.

Prevention activities include activities that are designed to avoid attack and limit the spread of infection. An example of cyber hygiene is safe browsing habits where dangerous phishing attacks, email attachments, and nefarious sites are avoided.

Active Monitoring refers to activities that offer an understanding of ongoing and near real time security status and early detection of threats.

Incident Response and Recovery refers to activities that respond to attacks or breaches once they occur. The goal is generally to contain and attack in order to limit a threat from spreading and placing other systems or people at risk.

Leadership/Operations refers to those activities that allow for collaboration and capacity building throughout the state.

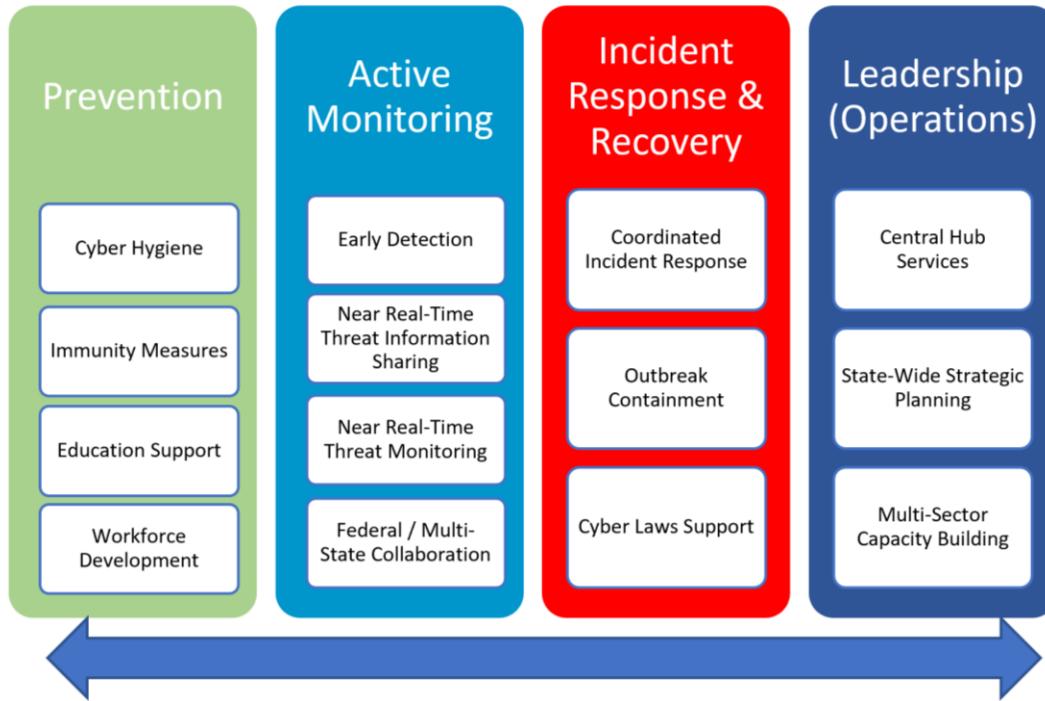


FIGURE 2: CYBERSECURITY ACTIVITY CATEGORIES

The CCoE has developed Divisions that each propose to offer a comprehensive array of programs that offer significant value for the state. The Divisions would take leadership for important functions of the CCoE. To ensure that the CCoE addresses the requirements established by Oregon law, Figure 3 on page 17 maps the fulfillment of the mission through the Divisions of the CCoE.³²

Figure 3³³ also illustrates the role of each Division in fulfilling the CCoE tasks. For example, all Divisions would contribute to operational tasks such as, creating the statewide strategic plans; acting as a central clearinghouse, or hub; and building capacity among different sectors. In those cases where a particular Division would not be directly involved in an activity, this is indicated by a horizontal dash.

The required tasks from the legislation are delegated and clearly accounted for among the Divisions of the CCoE. This approach aligns programmatic areas with the CPS Phase I research, foundational documents, OCAC contributions, and legislative intent. The tasks and role of each Division are further detailed in Section 5 of this Plan.


Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
 <p>CCoE Division ↓</p>														
Threat Information Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓
Education & Workforce Development	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Outreach and Awareness	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
Operations	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 3: CCoE STATUTORY TASK BREAKDOWN BY DIVISION

SECTION 4 – CCOE GOVERNANCE STRUCTURE

4.1 PROPOSED GOVERNANCE STRUCTURE

The CCoE is proposed to be governed by a board of directors using a reporting structure exemplified by Figure 4, below. The CCoE Board of Directors will establish bylaws that outline to what degree and by what formal process it will coordinate with OCAC; what roles individual members of OCAC may play in the CCoE oversight structure; and the CCoE’s official organizational status. The bylaws will also outline the role of the CCoE in executing state-mandated activities. The Board of Directors would provide oversight to the CCoE Executive Director, who is attached to the Operations Division. The CCoE Divisions are proposed to report to the Executive Director.

4.2 PROPOSED CCOE ORGANIZATIONAL STRUCTURE

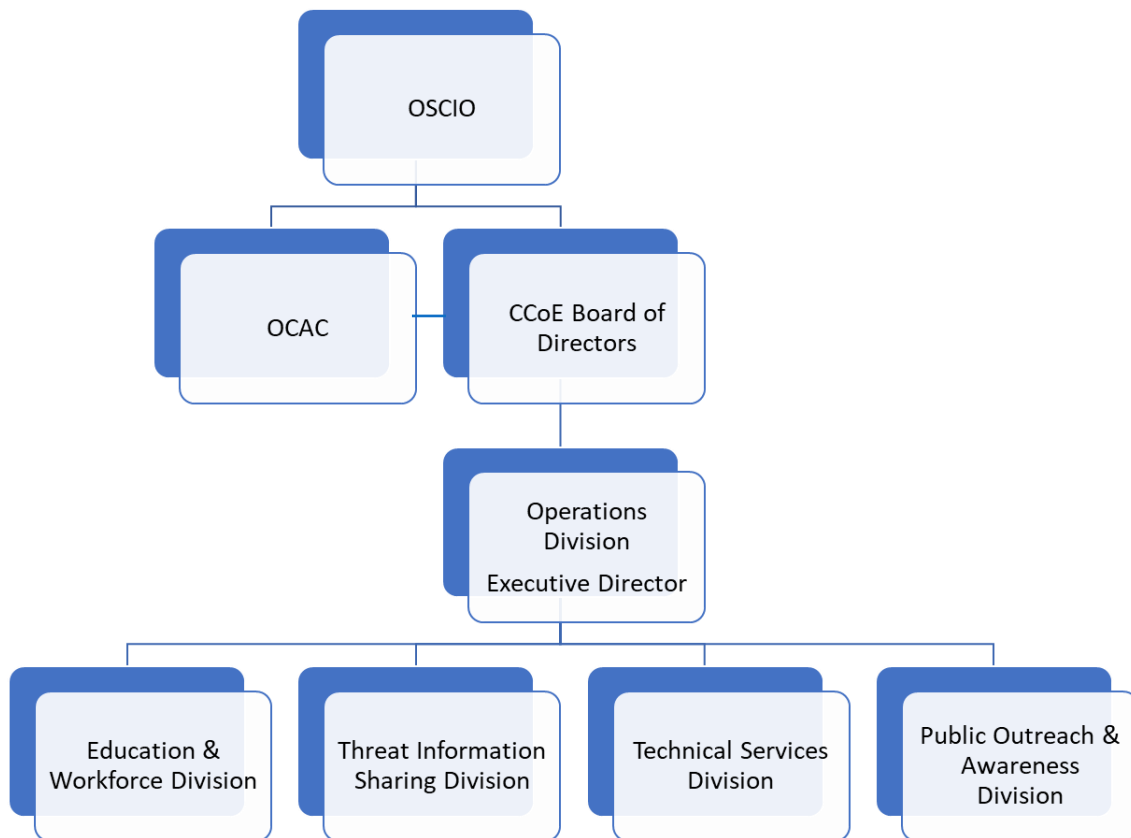


FIGURE 4: PROPOSED ORGANIZATIONAL CHART

SECTION 5 - CCOE DIVISION AREA PROGRAMMATIC PLANS

The following section outlines the programmatic plans of the CCoE, covering the four key Divisions: Operations; Education and Workforce Development; Threat Information Sharing; Technical Services; and Public Outreach and Awareness.

Each CCoE Division has framed its work to take a collaborative approach with the idea that leveraging existing resources and programs is most efficient and effective. In some cases, the CCoE intends to fill a gap, such as providing coordination and information sharing. In other cases, the CCoE proposes to develop partnerships in which the Division can support and enhance existing programs. In all cases, the CCoE intends to partner with public, private, and nonprofit organizations across the state.

Descriptions of each possible programmatic area include the following:

- Program area overview
- Division tasks and alignment with legislative requirements (SB90)
- Possible operational partners & companion resources

5.1 OPERATIONS DIVISION

5.1.1 OPERATIONS DIVISION OVERVIEW

The Operations Division proposes to provide the leadership necessary to build out the CCoE. Its primary functions include addressing the statutory requirements for state-wide strategic planning; CCoE Division oversight; multi-sector collaboration; and oversight and logistical support for the development of policy, financial, legal, and procurement matters. This Division provides a high value for the State in that it will leverage and coordinate resources in a way that is currently not possible. In the first phase, Operations will likely be the sole division. This Division will guide the establishment of all other Divisions that will then be responsible for implementing the programmatic plans as funding becomes available.

The Operations Division proposes to hire an Executive Director (ED) with minimal support staff to begin the immediate planning and development actions of the CCoE. This position will be responsible for drafting and delivering the Oregon Cybersecurity Strategy and a Cyber Disruption Response Plan and/or delegating, procuring, contracting, or to support the state-wide planning process. In addition, the ED will be responsible for public affairs and policy, finance & budgeting, and legal decisions.

5.1.2 OPERATIONS DIVISION TASKS AND ALIGNMENT WITH SB90

The tasks of the Operations Division are shown in Figure 5: Statutory Requirements - Operations Division, below. This graphic provides an overview of the Division's role in the CCoE. The graphic represents those activities that correspond to statutory requirements and those that correspond to supporting internal CCoE operations.

For example, Task A activities required by SB90 are related to strategic planning. Task B activities are accomplished by providing administrative support to CCoE Divisions as they roll out their programs. Where the Division does not lead on a particular role, the Figure indicates a horizontal dash.

Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
 CCoE Division ↓	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
	Threat Information Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓
Education & Workforce Development	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Outreach and Awareness	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
Operations	B	—	A	A	—	B	—	A	—	—	D	B	A	B
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 5: STATUTORY REQUIREMENTS - OPERATIONS DIVISION

SB90 Task A: Draft and biennially update the Oregon Cybersecurity Strategy and a Cyber Disruption Response Plan. These plans are to be submitted to the Governor and an appropriate committee or interim committee of the Legislative Assembly. The Cyber Disruption and Response Plan must include those elements listed in Appendix B.

To accomplish Task A, the Division is expected to actively seek and consider public input on cybersecurity policies and initiatives from impacted communities. This includes the need to:

- Coordinate among partners and the CCoE Divisions
- Engage with high-level multi-sector stakeholder, partner, beneficiary, governments, and constituencies. Target audiences include K-12 and higher education; private industry; small businesses, nonprofit agencies; state, local, and tribal governments; law enforcement agencies; OCAC; OSCIO; and others.
- Advise the State of Oregon on Cybersecurity Matters in coordination with OCAC and OSCIO³⁴

SB 90 Task B: Task B involves supporting the planning and execution of all CCoE tasks, which requires attention to issues of policy, financial, legal, and procurement best practices. These activities include the following tasks:

- Complete CCoE operational business plan
 - Incorporate a strong CCoE mission and purpose of public benefit, accountability, diverse involvement, and transparency into the business plan.
 - Meet face-to-face with members of communities outside of population centers who should feature prominently in any plans for further information gathering by CCoE decision makers
- Generate resources in conjunction with CCoE Divisions and other partners;
- Coordinate and manage budget and revenues for the CCoE;

- Engage with high-level stakeholder, partner, beneficiary, and funding opportunities;
- Provide oversight for CCoE program area plans including developing robust measurement, evaluation and transparency of CCoE Divisions and programs to help measure and illustrate the public benefits and value created by the CCoE;
- Develop and utilize best practices in procurement, policy, financial and legal issues

5.2 EDUCATION AND WORKFORCE DEVELOPMENT DIVISION

5.2.1 EDUCATION AND WORKFORCE DEVELOPMENT DIVISION OVERVIEW

The planned activities of the Education and Workforce Development Division are designed to expand cybersecurity education programs, increase access to educational materials, expand employee training, and grow the size and talent of Oregon’s cybersecurity workforce.

Cybersecurity professionals coupled with the rapidly growing demand for them, place severe constraints on the ability of organizations in Oregon to attract and maintain a qualified cybersecurity workforce. As shown in the Phase I research, other states are already capitalizing on this opportunity and are using cybersecurity as an economic driver. This Division would facilitate partnerships between industry and educational institutions to increase opportunities for students and professionals in cybersecurity. The school-to-work pipeline is especially integral and extends far beyond university programs and certifications to reach deeper into the K-12 system in order to begin creating the next generation of cybersecurity professionals while increasing cybersecurity awareness among communities.

This Division will work closely with other CCoE programs. For example, the Security Operations Center (SOC), information sharing (ISAO), and managed security services (MSSP) program areas all have significant educational components. This Division proposes to coordinate with the Public Outreach and Awareness Division to identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public’s personal information.

Student opportunities for internships and real-world experience would be a central feature of the SOC and other programs. Ideally, CCoE regional MSSPs could also include similar learning opportunities, making these opportunities more accessible to all Oregon students engaged in the cybersecurity field.

The Division also has an opportunity to partner with the Oregon Veterans Cybersecurity Initiative, a plan to deploy a “SWAT team” of veterans who would work directly with other veterans to identify where they can apply their interests and service experience in cybersecurity-related career tracks. The goal is to help connect these veterans with institutions in Oregon who are hiring cybersecurity professionals.

5.2.2 EDUCATION AND WORKFORCE DEVELOPMENT TASKS AND ALIGNMENT WITH SB 90

The Education and Workforce Development program area of the CCoE plays a significant role fulfilling the tasks envisioned by SB90. Figure 6, below also provides an overview of the Division’s role within the CCoE.

FIGURE 6: STATUTORY REQUIREMENTS – EDUCATION AND WORKFORCE DEVELOPMENT DIVISION

Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
<p>CCoE Division ↓</p>	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
Threat Information Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓
Education & Workforce Development	D	C	B	B	A	A	A	D	A	A	D	A	C	C
Public Outreach and Awareness	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
Operations	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The Education and Workforce Development Division has identified a number of programmatic concepts, some of which are currently operating in pilot or small forms, that through (or with the assistance of) CCoE efforts could be significantly expanded. Exemplary concepts appear in Appendix A. These include the following:³⁵

SB 90 Task A: Support Educational Components of CCoE Divisions. The Education and Workforce Division proposes to support other Divisions in cybersecurity incident response and cybercrime investigations by participating in a Teaching SOC and facilitating internships. The SOC would increase access to response and recovery assistance for cyber disruptions and investigations. One way to view this initiative would be as a partnership with the SOC to establish a “cybersecurity teaching hospital”

SB 90 Task B: Workforce Development. The Division would encourage the development of the cybersecurity workforce through a number of measures including, but not limited to, competitions aimed at building workforce skills; disseminating best practice; and facilitating cybersecurity research and encouraging industry investment and partnership with post-secondary institutions of education and other career readiness programs in order to increase numbers of qualified cybersecurity professionals in Oregon. These activities may include:

- Support for the Veterans SWAT team
- Facilitate structured mentorship programs, including partnering with Oregon Pathways Project, which seeks to guide future security professionals along their development path from youth-focused programs through internships and apprenticeships to establish them in the workforce.

- Support cybersecurity internships
- Facilitate and support partnerships among public, private, and nonprofit agencies that supply academic-to-employment tracks
- Research and develop preventative training programs
- Design and support retraining efforts for non-veteran Workforce participants at high risk of being displaced by automation, disability, or family care responsibilities

SB 90 Task B: Education and Training. This area focuses on facilitating the development of K-12 and higher education initiatives, including cyber hygiene and computer science education in Oregon. This focus should be part of both the initial CCoE offerings and the long-term cybersecurity strategic plan. This includes the following proposed activities:

- Facilitating or partnering to support extra-curricular and K-12 cybersecurity educational programs
- Develop curricula and programs for technical and non-technical audiences
- Supporting access to computer science and cybersecurity related student competitions
- Expanding access to NW Cyber Camp
- Recommend content and timelines for conducting cybersecurity awareness training for state agencies and the dissemination of educational materials to Oregon’s public and private sectors;
- Develop strategies for collaboration with the private sector and educational institutions through the CCoE and other venues to identify and implement cybersecurity best practices
- Developing K-12 student and teacher computer science capacity and literacy-building tools and partnerships

SB90 Task C: Planning, Capacity Building, and Prevention. The Division proposes to assist in the development of the state-wide strategic planning processes, and support capacity building programs. These efforts can take several forms, including:

- Assisting organizations to align training programs with cybersecurity needs
- Disseminating research and best practice results to Oregon’s public and private sector organizations for practical use and guidance

SB90 Tasks D: Incident Response and Recovery. This Division proposes to support incident response and recovery by collaboratively identifying and participating in appropriate federal, multistate or private sector programs and efforts that support or complement the center’s cybersecurity mission. In particular these include:

- Support for cybersecurity research by facilitating grant notifications and opportunities and dissemination of results
- Encouragement of multi-sector industry investment in educational programs and facilitation of partnerships with post-secondary institutions of education and other career readiness programs³⁶

5.2.3 POSSIBLE OPERATIONAL PARTNERS & COMPANION RESOURCES

The Education and Workforce Division proposes to work with partners across the state of Oregon in the fulfillment of its tasks. As noted later in this Plan, Oregon State University has committed resources to serve as

the CCoE MSSP. These potential partnerships span multiple sectors and key entities include but are not limited to:

- Higher education institutions (MHCC, OSU, Oregon Tech, PSU, UO, OHSU, PCC, RCC, LCC, SOU etc.)
- MHCC Center for Academic Excellence Cybersecurity & Networking Program
- K-12 Academic Institutions
- Oregon Fiber Partnership
- OR TITAN fusion center collaboration
- Cybersecurity Industry
- Computer Science Industry
- ISAO Network partners from Threat Division
- DHS/FBI/DOJ/State Police
- Critical Infrastructure Owner/Operators
- National Guard
- Oregon Veterans Cybersecurity Initiative
- NW Cyber Camp
- OSU ORTSOC initiative
- The State of Oregon
- Oregon Cyber Pathways Project

5.3 THREAT INFORMATION SHARING DIVISION

5.3.1 THREAT INFORMATION SHARING DIVISION OVERVIEW

The Threat Information Sharing Division would be responsible for the CCoE Information Sharing and Analysis Organization (ISAO). It would be responsible for collaboration and state-wide engagement concerning cybersecurity information sharing of best practices. The Division proposes to support near real-time information sharing about cybersecurity threats, breaches, and trends among national, regional, and multistate entities, and within Oregon among the public and private sectors. The ISAO proposes to support communities of interest that include urban and rural, sector-specific and regional ISAOs, owners and operators of critical infrastructure, relevant state and federal agencies, academic institutions, and other public- and private-sector stakeholders.

The ISAO program concept is in early development and will require additional analysis to identify the sequence and best strategies for the most effective implementation. However, the ISAO function is premised on an understanding that it will require significant partnerships and a voluntary and consensus-based process for it to maximize its effectiveness.

The establishment of a CCoE ISAO would allow communities of interest to share cyber threat information with each other on a voluntary and confidential basis, emphasizing the need for mutual trust and transparency carefully balanced with confidentiality in participation.

5.3.2 THREAT INFORMATION SHARING TASKS AND ALIGNMENT WITH SB90

The Information and Threat Sharing programs are proposed to provide support for the CCoE and its Divisions in the areas of Prevention, Active Monitoring, Incident Recovery & Response, and Leadership. Figure 7 provides an overview of its role in the CCoE. The graphic is a representation of those activities that correspond to the statutory requirements.

Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
<p>CCoE Division ↓</p>	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
<i>Threat Information Sharing</i>	B	B	C	C	A	A	A	A	B	B	—	A	C	C
<i>Education & Workforce Development</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>Public Outreach and Awareness</i>	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
<i>Operations</i>	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
<i>Technical Services</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 7: STATUTORY REQUIREMENTS - THREAT INFORMATION SHARING DIVISION

SB90 Task A: Active Monitoring. This Division intends to serve as an ISAO pursuant to 6 U.S.C. 133 et seq., and as a liaison with the National Cybersecurity and Communications Integration Center within the United States Department of Homeland Security, as well as work with other federal agencies and public and private sector entities in Oregon. It plans to coordinate cybersecurity information sharing (Threat Intelligence) and promote shared and real-time situational awareness between the public and private sectors throughout the state.

Many of these activities represent the procedural predecessors to establishing an ISAO, which would be completed in the first 6 months of CCoE operation. These activities include:

- Maintain and monitor a consensus-based standards development process for threat intelligence sharing. These include but are not limited to contractual agreements including non-disclosure and non-attribution agreements, business processes, operating procedures, technical specifications, and privacy protections;
- Write internal CCoE Information Sharing and Analysis Organization Plan proposal;
- Participate in existing federal cybersecurity information sharing programs.

SB90 Task B: Incident Response and Prevention. The goal of this Division is to coordinate information sharing regarding cybersecurity risks and incidents across all types of organizations and provide a statewide forum for discussing cybersecurity issues. This will include coordinating with public awareness activities in the context of a statewide forum for discussing and resolving cybersecurity issues. Some activities may be conducted in collaboration with the Public Outreach and Awareness and Incident Response & Recovery Division. These activities may include:

- Face-to Face engagement state-wide through Cyber summits, breakfast, luncheon, and town hall type events, especially in rural areas
- Conferences and activities targeted at a technical audience
- Provision of information and recommended best practices concerning cybersecurity and resilience measures to public and private entities utilizing the CCoE website and public outreach activities
- Collaborative efforts focused on education and workforce development opportunities

SB 90 Task C: Prevention and Leadership. This Division will also work to identify and participate in appropriate federal, multistate or private sector programs and efforts that support or complement the CCoE’s cybersecurity mission. Activities would include:

- Participation in existing federal cybersecurity information sharing programs. Examples include: MS-ISAC, NCCIC within Dept. of Homeland Security, FBI, State Police, Oregon Fusion Center, etc.
- Support for statewide strategic planning efforts
- Support for multi-sector capacity building through pursuing diverse involvement in the ISAO

5.3.3 POSSIBLE OPERATIONAL PARTNERS AND COMPANION RESOURCES

The Threat Information Sharing Division will work with partners across the state of Oregon collaboratively in the fulfillment of its tasks. The OCAC Information Sharing Division has received a commitment from The University of Texas San Antonio (USTA) which is the home of ISAO.org, an extensive resource created exactly for the purpose of setting up ISAO’s. They are available to consult with the CCoE and OCAC at no cost. They are also willing to conduct on-site workshops and provide the framework and blueprints to insure the success of this effort.

A variety of Oregon’s academic institutions have all shown interest in participating and possibly sharing or contributing space or resources to this endeavor.

Additional potential partners include:

- | | | |
|---|---|---|
| • OR Titan Fusion Center | • Multi-State Information Sharing and Analysis Center (MS-ISAC) | • Academic Institutions |
| • National Cybersecurity and Communications Integration Center (NCCIC) and other Department of Homeland Security programs | • Regional and Sector-specific ISAOs (Financial, Health, Social, adjacent states) | • FBI, DOJ, State Police |
| | | • Oregon Fiber Partnership |
| | | • ISAO.org at the University of Texas San Antonio |
| | | • BSIDES Portland |

5.4 TECHNICAL SERVICES DIVISION

5.4.1 TECHNICAL SERVICES DIVISION OVERVIEW

The Technical Services Division is designed to provide technical expertise across the entire CCoE. The Technical Services Division would coordinate public cybersecurity services, technical controls, cyber incident response, and threat intelligence sharing.

This Division is uniquely structured with a built-in advisory function provided by OCAC. OCAC leadership is working to create a Technical Services Advisory Committee in order to provide more permanent technical program support, specifically for the responsibilities of this division. The Technical Services Advisory Committee will be a dedicated resource provided by OCAC that the CCoE can utilize for the following operational support functions as detailed in the activities section below.

5.4.2 TECHNICAL SERVICES DIVISION TASKS AND ALIGNMENT WITH SB90

The Technical Services program is intended to provide support for activities across the CCoE Divisions (see Figure 8 below which provides an overview of its role within the CCoE).

The Division’s tasks are not specifically labeled in correlation with the SB 90 requirements because, unlike other Divisions, Technical Services has numerous roles to play across the CCoE, including support, technical advisory, and services centralization.

Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
<p>CCoE Division ↓</p>	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
Threat Information Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓
Education & Workforce Development	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Outreach and Awareness	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
Operations	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 8: STATUTORY REQUIREMENTS - TECHNICAL SERVICES DIVISION

The following activity areas are outlined for the Technical Services Division:

OCAC Technical Advisory Committee: OCAC leadership is concurrently creating a Technical Advisory Committee designed to provide more permanent program support. The Technical Services Advisory Committee proposes to be a resource for the following operational support roles:

- Supporting the CCoE in its role of advising the State of Oregon on cybersecurity and IT security issues
- Providing input, guidance, and review concerning technical aspects of CCoE program proposals, and the State Strategy and Disruption Plan and Statewide Cybersecurity Strategic Plans required under SB 90
- Serving as the content and technical committee that reviews materials and programs for collaborating partners and across CCoE Divisions
- Serving as part of the Cybersecurity Expert Speaker placement program for the Public Outreach Division and assisting with public education events where technical spokespeople may be needed
- Assisting in the review and development of technical requirements or proposal criteria, website content, educational materials, and workforce training materials
- Providing technical input to other working groups as needed
- Providing advising, technical review, and consulting support where appropriate

MSSP Program Area: The Division proposes to provide oversight and coordination of the Managed Security Services Provider (MSSP) program. The MSSP envisions providing low-cost cybersecurity support to underserved organizations.³⁷ The MSSP would work with organizations throughout the state that are unattractive for commercial cybersecurity companies due to their lack of funding, remote locations, or lack of awareness. The MSSP envisions a partnership with Oregon colleges in which students would provide services, under the instruction and supervision of faculty and professional advisors. In this way, the MSSP concept would offer students real-world experience that would support educational programs and grow the cybersecurity workforce.

The target audience may include such organizations such as: K-12 districts, small businesses (e.g., financial, legal, health, farms, and non-profit organizations). The nature of these organizations makes serving them unprofitable for commercial business. Yet often, these organizations become targets of cybercrime because they store personal information, have financial assets that can be stolen, and computation assets that can be ransomed.

The MSSP will develop standards and policies to ensure that it does not compete with private sector providers engaged in similar activities. The services of the MSSP would support and compliment the activities envisioned by the SOC and ISAO. In summary, the following activities are proposed:

- Provide Managed Security Services to underserved populations, such as farms, minority owned, women owned and veteran owned businesses
- Provide Triage Teams in coordination with the SOC and ISAO
- Offer referrals to other resources or law enforcement
- Partner with the Public Awareness and Outreach Division of the CCoE to teach and educate those who may lack cybersecurity awareness

5.4.3 POSSIBLE OPERATIONAL PARTNERS & COMPANION RESOURCES

The CCoE Technical Services Division will work with potential partners across the state of Oregon collaboratively in the fulfillment of its tasks. Future activities planned as part of the Cybersecurity Statewide Strategic Plan will identify additional partners that are likely to collaborate on contributing, raising, or sharing resources.

Additional partners include the following:

- Academic Institutions (K-12)
- Higher Education Institutions (MHCC, OSU, Oregon Tech, PSU, U of O, OHSU, OR Fusion IT,
- Center, PCC, RCC, LCC, SOU)
- Oregon Fiber Partnership
- OR TITAN Fusion Center
- Cybersecurity Industry
- OSU ORTSOC
- Small Business Development Centers
- Small Business Associations

5.5 PUBLIC OUTREACH AND AWARENESS DIVISION

5.5.1 PUBLIC OUTREACH AND AWARENESS DIVISION OVERVIEW

The planned activities of the Public Outreach and Awareness Division are designed to promote cybersecurity awareness and increase access to CCoE resources, experts, tools, and educational materials. The Division would accomplish this through digital marketing, content marketing, event marketing, earned media, public relations, paid media and advertising.

5.5.2 PUBLIC OUTREACH AND AWARENESS TASKS AND ALIGNMENT WITH SB90

The Public Outreach and Awareness program proposes to provide support for the CCoE and its Divisions in the areas of Prevention, Active Monitoring, and Leadership. Figure 9, below, provides an overview of its role in the CCoE.

Statutory Framework →	Prevention				Active Monitoring				Incident Response & Recovery			Leadership		
<p>CCoE Division ↓</p>	Cyber Hygiene & In-Person Events	Immunity Measures	Education Support Initiatives	Workforce Development Initiatives	Early Detection	Near Real-time Threat Info Sharing	Near Real Time Threat Monitoring	Federal and Multi-state Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws Support & Development	Central Hub Services & Division Leadership	State-Wide Strategic Planning	Multi Sector Capacity Building
Threat Information Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓
Education & Workforce Development	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Outreach and Awareness	A	B	C	C	—	—	—	D	—	—	—	A	A	D
Operations	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 9: STATUTORY REQUIREMENTS - PUBLIC OUTREACH & AWARENESS DIVISION

SB90 Tasks A & B: Prevention and Leadership. Tasks A and B involve coordinating information sharing regarding cybersecurity risks and incidents across all types of organizations³⁸ and providing a statewide forum for discussing issues.³⁹ This would also include public awareness activities that ensure identification of the CCoE as a resource for public, private, and nonprofit agencies, as well as the general public. These activities include the following:

- Develop and deliver strategic marketing campaigns and programs, including implementing a branding strategy for CCoE and components and building out the CCoE website as a cornerstone resource for coordinating and communicating core activities

- Coordinate a messaging strategy for CCoE, grounded in its goals and top priorities
- Promote engagement for each of the adjoining Division missions and the CCoE, including multi-sector marketing events, and monthly and yearly conferences throughout the state
- Develop public awareness programs to facilitate access to information that would help Oregon businesses and organizations improve cybersecurity

SB 90 Task C: Prevention. Task C involves encouraging cybersecurity workforce development initiatives.⁴⁰ The Public Outreach and Awareness program area proposes to serve as an important link between the CCoE’s workforce development activities and other Divisions. The goal is to help ensure that educational and workforce development opportunities are effectively promoted throughout Oregon in a wide variety of venues and organizational networks. An especially important component of this effort would be partnerships with K-12 and higher education institutions to share and coordinate activities.

SB90 Task D: Capacity Building. Task D involves participating in appropriate federal, multistate or private sector programs and efforts that support or complement the center’s cybersecurity mission, including the opportunity to:⁴¹

- Promote legislative initiatives
- Create and maintain a Cybersecurity “Expert Speaker” placement program
- Share lessons, resources, stories, and expertise g through various communications channels such as newsletters, social media and earned media (e.g. news articles) and paid media throughout the state
- Conduct research about how to improve the program’s effectiveness using evaluation metrics on increased cybersecurity awareness, including impressions, website traffic, number of social media followers and level of engagement, event attendance, and search rankings

5.5.3 POSSIBLE OPERATIONAL PARTNERS & COMPANION RESOURCES

The CCoE Public Awareness & Education Division will work with partners across the state of Oregon collaboratively in the fulfillment of its tasks.

These partners are identified as follows:

- | | | |
|--|--------------------------------------|---|
| • Rural area regional chambers of commerce | • Small Business Development Centers | • Public agencies, Including State, City, and County, and Tribal leadership |
| • County extension offices | • Special districts | • School districts |
| | • Cybersecurity Industry | • Higher Education |

SECTION 6 - TIMELINE OVERVIEWS & IMPLEMENTATION PHASING

This section outlines the proposed phasing strategy for establishing the CCoE (see Table 2 below). Implementation of these phases depend on the funding available.

Phase I covers the timeframe of October 1, 2019-June 30, 2020. Phase II covers the timeframe of July 1, 2020-June 30, 2021. Phase III covers the timeframe of July 1, 2021 and beyond. The timeline expresses Phase I action items in quarters (Q), Phase II actions in 6-month increments (H) and Phase III actions in years (Y). As the timeframe moves out into later years, the ability to phase actions is less specific.

TABLE 2: CCOE PHASING STRATEGY

	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*			

*some programs may allow for ongoing monitoring and evaluation

As roll-out of the CCoE continues along this timeline, the Center would establish a cyclical process of strategic planning, programmatic development, and monitoring and evaluation. The improvement of Oregon’s cybersecurity strategies should be iterative and strengthen the state’s cybersecurity posture with each cycle, building on success, providing adjustment to any roadblocks that might emerge, and delivering timely and transparent evidence of progress against established benchmarks and goals.

SECTION 7 - BUDGET, FINANCIAL RESOURCES, AND POTENTIAL PARTNERS

7.1 BUDGET NARRATIVE

The budget shows the estimated funding needs for each proposed CCoE Division. It includes the statewide strategic planning and establishment costs in the Operations Division. The budget distinguishes between those activities that are required by ORS276A.326-29, and those that would fund other planned activities.

The budget to fund the required statewide planning efforts would be \$1,665,000 over two fiscal years. To fully fund the programmatic plans, would require an additional \$9,331,633. The CCoE is aware that the legislative appropriations process involves a certain element of uncertainty; this effort must be prepared with funding contingency plans.

As a result, this budget is illustrative and based on fully funding all of the concepts proposed. However, programs and priorities may change or overlap based on the findings of the statewide strategic planning effort and/or funding availability. Ultimately, there should be flexibility to elect those programs and phases necessary to achieve the goals of the CCoE. Additionally, Division budgets may be scaled up or down, depending on the phasing strategy and funding availability. Therefore, the resources from a variety of funding sources and those detailed in the funding strategy sections of this Plan will be important to consider.

The proposed budget for the CCoE includes funds to implement Phase I and II activities and beyond.

7.2 BUDGET

The budget that appears in Table 3 is organized into the CCoE’s proposed phases. These activities include the establishment of the CCoE, the creation and filling of an Executive Director position, and minimal support staff to begin implementing the immediate administrative and planning actions of the CCoE. Phase I also includes the funds necessary to begin the immediate Disruption Response and Strategic Cybersecurity planning for the State of Oregon, as required by ORS 276A.326-9. Additional funding for CCoE programmatic plan implementation appears in Phase 2 and Phase 3, both of which are estimated and depend on funding availability. These programmatic plans appear in Section 5 earlier in this Plan.

TABLE 3: CCOE PROPOSED ILLUSTRATIVE BUDGET BY PHASE

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
TOTAL		\$760,000.00	\$4,682,559.00	\$5,554,074.00	\$10,996,633.00

7.3 FUNDING STRATEGY

In order for the CCoE to make a state-wide impact, it will require significant funding in the order of magnitude as described in the plan. If core or seed funding is not available from state sources, the efforts of the CCoE are likely to be delayed and jeopardized. As a result, the OCAC will be required to expedite its funding search from other outside sources. This too may prove to be problematic, given the unlikelihood of grant sources that will fund start-up organizations. Nevertheless, there are grant opportunities that would be appropriate to fund the programs described in this Establishment Plan.

7.3.1 GRANT OPPORTUNITIES

This section is supported by a more detailed funding summary that appears in Appendix C. The Appendix is a comprehensive list of opportunities that may be pursued to accomplish the goals of the Oregon Cybersecurity Advisory Council (OCAC) and the Oregon Cybersecurity Center of Excellence (CCoE)⁴².

The summary includes government and foundation sources that provide support for programs. It does not include smaller in-kind donations or sponsorships that the CCoE can pursue to support conferences or websites, nor does it include fees for services that CCoE might generate for its services and expertise once established.

Consistent with the goals of the CCoE, the majority of the activities for which funding is available are focused on education and workforce development. Owing to the diversity of grant purposes, the collaborative feature of the CCoE is beneficial, as this approach can increase opportunities for funding eligibility. For example, where some grants are only available to institutions of higher education, others are targeted at nonprofit organizations. Partnerships can therefore expand the overall programming support available.

Appendix C provides a crosswalk of grant opportunities organized by the following categories: Funding entity, funding opportunity and description, alignment with SB90, access/links for more information, application window / deadline, and funding range/past grants in Oregon, and proposer specifications.

7.3.2 FEDERAL FUNDING

The National Science Foundation (NSF) offers the majority of the relevant funding opportunities for cybersecurity initiatives that are aligned with the functions statutorily assigned to the CCoE and/or OCAC. Of the thirteen (13) grants identified as being aligned with the CCoE, eleven (11) are programs of the NSF. Many of these grants focus on workforce and economic development, and a number of them target economic development activities in rural areas. Homeland Security provides one opportunity to fund “target hardening” and cybersecurity training for nonprofit staff. Current grants offer support for the following activities:

- Higher education technology infrastructure updates, paired with research opportunities for students
- K-12 STEM education
- Training and education for scientific and engineering workforce development
- Career pathways/technician education
- Broad economic development activities, including “technology-based economic development”

The CCoE should prioritize its initial funding requests to education and workforce development, as well as potential opportunities for CCoE organizational support (see the Cybersecurity Innovation for Cyberinfrastructure (CICI). In addition, the CCoE may facilitate a minimum of one institution of higher education becoming a host cite for CyberCorps scholarships. CyberCorps (Scholarships for Service) provides direct support to university students in cybersecurity programs, followed by public service obligations. This program will fill a unique niche nationally, as it is not yet available at any Oregon institution.

7.3.3 FOUNDATION AND PRIVATE SOURCES

Appendix C lists fifteen (15) possible foundation funding opportunities that are aligned with the OCAC and CCoE. As with federal grants, education and workforce development are prioritized. The funders in Appendix C represent opportunities ranging from \$1,000 up to \$75,000. The majority of foundation funders explicitly require a 501(c)(3) designation from the IRS. Depending on the grant, some further specify the types of entities that may apply, such as a library or school.

7.3.4 MEMBERSHIP OR SERVICE FEES

The CCoE may rely, in part, on membership fees or fees for service. While many of the Divisions would likely require additional support, membership or service fees may offset the public and private funds otherwise needed to operate core programs. This approach especially might be applicable to the CCoE MSSP, ISAO, and other select divisions and activities.

While membership fees and fees for service may be critical for ongoing operational support of programs, they can be difficult to obtain prior to service availability. While important for ongoing program support, these revenue sources will not be applicable to address the needs for substantial startup capital and initial expenses, nor for certain types of programs such as general public awareness building.

7.3.5 OTHER FUNDING VEHICLES

There may be other opportunities for funding that would require significant development and consideration. For example, one viable strategy might be a tax credit for donations dedicated to the Cybersecurity Fund. However, in today's political and budgetary climate, this would possibly represent a very long-term process and could not be relied upon as a source of funding.

7.3.6 FUNDING STRATEGY SUMMARY

While several federal and private grant programs have the potential to provide significant funding for the CCoE and its core programs, these funding opportunities are highly competitive. To be competitive for such grants and other funding, it's important that the CCoE quickly establish a track record of proven success. Without a base of core funding for the CCoE, it will be difficult to pursue this approach. In addition, the small size of most private grants makes doubtful the wisdom of relying on such sources as a general strategy. Instead, private grants should be considered for stop gap, supplemental, or early activities/pilots only.

That said, there a number of grant sources, as outlined in Appendix C, that are clearly aligned with the CCoE and its proposed programs. Given a sufficient base level of initial support from public funds, the CCoE has the potential to be successful in this area.

7.4 PARTNERSHIPS & SHARED RESOURCES

7.4.1 PROPOSED OPERATIONAL PARTNERS & COMPANION RESOURCES

Effective and efficient cybersecurity is highly interdependent and collaborative. Through OCAC and the OSCIO leadership, the CCoE envisions that a core function of its work will be in facilitating collaboration among the public, private, and nonprofit sectors, and organizations. At the outset, each Division has identified a set of likely partners. However, over time, the CCoE intends that its facilitative activities create a network of sustained engagement. Given some initial funding and core support, the CCoE has enormous potential to leverage additional resources from this network for significant additional impact.

Table 4, below, maps the initial relationship among these resources. For some Divisions, these partnerships represent opportunities to share resources and collaborate. For other Divisions, these partners may offer networking activities. The term “Operational Partner” indicates that the Division proposes to delegate or substantially share in delivering services or activities. The term “Companion Resource” indicates that the Division will coordinate, network, or share information with these entities.

TABLE 4: PROPOSED OPERATIONAL PARTNERS AND COMPANION RESOURCES

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

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

7.4.2 COMMITTED RESOURCES

To date the CCoE has committed resources to the establishment of the CCOE by offering to expand its Oregon Research and Teaching Security Operations Center (ORTSOC) to serve as its MSSP.

OSU is dedicating 0.5 FTE of the full-time ORTSOC Director, 1.0 FTE from our ORTSOC dedicated full-time security analysts, and approximately 0.5 FTE from several part-time student analyst positions to these efforts. Additionally, OSU is providing the requisite space for hosting ORTSOC and its growing staff.

SECTION 8 - PUBLIC VALUE MEASUREMENT AND EVALUATION

As part of establishing the CCoE, an evaluation and monitoring plan is proposed. The final evaluation plan should be modified, scaled and applied at the Division and programmatic area levels. This will aid the CCoE to monitor for effectiveness and ensure budgetary and statutory compliance.

Evaluation and ongoing monitoring of program outcomes and impact should capture the key areas of education, workforce, and mitigation of the impacts of cyber-attacks.

Education and Workforce Development

- Increased numbers of qualified cybersecurity professionals
- Increased connection to workforce pathways for Oregon students
- Increased Veteran participation in the cybersecurity workforce
- Trustworthy and transparent centralized information sharing system for Oregonians based on consensus driven standards and focused on mutual trust and privacy

Community Engagement and Education

- Increased coordination among a wide network of engaged organizations
- Increased visibility of and participation in Oregon's community-based cybersecurity expertise and preparedness
- Increased awareness and visibility of threats and opportunities across Oregon for cybersecurity business and educational programs, workforce availability, and companies
- Increased state employee cyber security awareness and capacity
- Increased awareness and visibility of preventative cybersecurity culture
- Increased access to immediate threat information, best practices, and opportunities for face-to-face engagement

Program Outputs

- Increased access to cybersecurity experts, cybersecurity education, and hands-on training
- Increased basic measures of protection in small and underserved organizations
- Reduced number of cyber incidents and losses due to cybercrime

Public Impacts

- Cost savings for individuals and businesses victimized by cyber attack or data breach
- Increased resilience to cyber threats
- Reduced time from data breach to detection and containment
- Increased State-Wide access to response and recovery assistance for cyber disruptions
- Increased capacity for small organizations to respond to and mitigate cyber crime

Establishing the CCoE, with its collaborative and complimentary approach, is an essential step to delivering important public value outcomes and impacts for all Oregonians.

ACKNOWLEDGEMENTS

The development of this Plan has involved the work of a many partners throughout Oregon. This process has involved the following persons, organizations, and entities. We would like to thank them for their participation and energy in this process.

Name	Organization
Aaron Farraiuolo	UpTime Sciences
Abrar 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	Revcaster
Isaac Potoczny-Jones	Tozny
Jack Estep	RSA
Jared Swezey	UpTime Sciences
Jason Adsit	Oregon National Guard
Jeff McJunkin	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

END NOTES

- ¹ Center for Public Service estimate of 89,469 small employers x 54% at risk of a breach x average cost of a breach of \$34,604 = approximately \$1,671,823,052.
- ² Portland State University Center for Public Service, Rebecca Jensen Craven, Jess Daly, and Elizabeth Gray. A Cross-Sector Capabilities, Resources, and Needs Assessment: Research to Support the Drafting of the Oregon Cybersecurity Center of Excellence Proposal. Report. December 2017. <https://www.pdx.edu/cps/sites/www.pdx.edu.cps/files/Cybersecurity%20Needs%20Assessment%20Final%20Draft.pdf>.
- ³ Oregon Office of the State Chief Information Officer. *Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon"* - Written Testimony for the Joint Legislative Committee on Information Management and Technology. December 12, 2016. p 10-15.
- ⁴ Oregon. State Legislature. Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence. 2017. <https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB90/Enrolled> . Section 3.
- ⁵ See also definition by United States CIO Council. "Continuous Monitoring." CIO.gov. Accessed December 16, 2018. <https://www.cio.gov/agenda/cybersecurity/continuous-monitoring/>.
- ⁶ Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment."
- ⁷ Oregon Office of the State Chief Information Officer, "*Unifying Cyber Security in Oregon.*"
- ⁸ Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.
- ⁹ Federal Bureau of Investigation Internet Crime Complaint Center. "2017 Internet Crime Report." 2017. https://pdf.ic3.gov/2017_IC3Report.pdf.
- ¹⁰ Viuker, Steve. "Cybercrime and Hacking Are Even Bigger Worries for Small Business Owners." The Guardian. January 21, 2015. Accessed December 16, 2018. <https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-america>
- ¹¹ Milkovich, Devon. "13 Alarming Cyber Security Facts and Stats." Cybint Solutions - A BARBRI Company. December 03, 2018. Accessed December 16, 2018. <https://www.cybintsolutions.com/cyber-security-facts-stats/>.; Mansfield, Matt. "Cyber Security Statistics: Numbers Small Businesses Need to Know." Small Business Trends. October 24, 2018. Accessed December 16, 2018. <https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html>
- ¹² Federal Bureau of Investigation IC3 Annual Report. <https://www.ic3.gov/media/annualreports.aspx>
- ¹³ Center for Public Service estimate of 89,469 small employers x 54% at risk of a breach x average cost of a breach of \$34,604 = approximately \$1,671,823,052.
- ¹⁴ Cyber Seek, "Cybersecurity Supply/Demand Heat Map." <https://www.cyberseek.org/heatmap.html>
- ¹⁵ Cyber Seek, "Cybersecurity Supply/Demand Heat Map."
- ¹⁶ Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment."
- ¹⁷ Oregon. State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.
- ¹⁸ Oregon Office of the State Chief Information Officer, "*Unifying Cyber Security in Oregon.*"
- ¹⁹ Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment," p. 15.
- ²⁰ Christian Leuprecht, David Skillicorn, and Victoria Tait, "*Beyond the Castle Model of cyber-risk and cyber-security,*" Government Information Quarterly 33, no. 2 (2016): 250-257.
- ²¹ Wojciech Mazurczyk, Szymon Drobniak, and Sean Moore, "*Toward a Systematic View on Cybersecurity Ecology,*" in *Combatting Cybercrime and Cyberterrorism*, ed. Babak Akhgar and Ben Brewster (Switzerland: Springer International, 2016), pg. 17-37.
- ²² Kristen Osenga, "*The Internet is Not a Super Highway: Using Metaphors to Communicate Information and Communications Policy,*" Journal of Information Policy 3 (2013): 30-54.

-
- ²³ Sedenberg, Elaine M., and Deirdre Mulligan. "Public Health as a Model for Cybersecurity Information Sharing." *Berkeley Technology Law Journal* 30, no. 2 (2015): 1737-9. Accessed September 05, 2017. doi:<https://doi.org/10.15779/Z38PZ>.
- ²⁴ Melissa, Hathaway, and Potomac Institute for Policy Studies. *The Cyber Readiness Index 2.0: A Plan for Cyber Readiness Baseline and Index*. Publication. November 2013. <http://www.potomacinstitute.org/images/CRIndex2.0.pdf>.
- ²⁵ Spidalieri, Francesca. "State of the States on Cybersecurity." The Pell Center. February 01, 2015. Accessed September 05, 2017. <http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/>
- ²⁶ Sedenberg, "Public Health as a Model for Cybersecurity Information Sharing."
- ²⁷ Figure 1 – Adapted from the Oregon Office of the State Chief Information Officer. *Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon"*, Adapted from - Jeff Rowe, Karl Levitt, and Mike Hogarth, "Towards the Realization of a Public Health System for Shared Secure Cyber-Space" (ACM Press, 2013).
- ²⁸ In addition, the plan must identify any grants, donations, gifts or other form of conveyance of land, money, real or personal property or other valuable thing made to the state from any source that is expected to support the establishment and continued operation of the center.
- ²⁹ Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment," p. 15.
- ³⁰ Not all participants responded to all survey questions posed as part of the study.
- ³¹ This percentage included those responding "Don't Know".
- ³² Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.
- ³³ Adapted from Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment," p. 15.
- ³⁴ Responsibility assigned to OCAC.
- ³⁵ Portland State University Center for Public Service, "A Cross-Sectoral Capabilities, Resources, and Needs Assessment."
- ³⁶ Responsibility assigned to OCAC.
- ³⁷ The MSSP concept incorporated a proposal submitted by the Oregon Institute of Technology.
- ³⁸ Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence, Section 4(1)
- ³⁹ Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence, Section 3(4)b
- ⁴⁰ Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence, Section 3(4)e
- ⁴¹ Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence, Section 4(4)
- ⁴² These 11 mandates and goals can be found in SB 90, Oregon State Legislature, Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence, Sections 3 and 4.