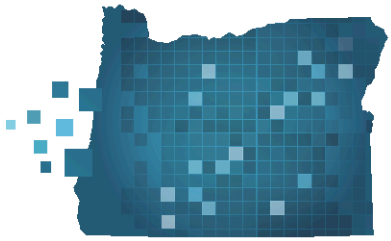


Oregon Cybersecurity Center of Excellence

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

CYBEROREGON

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*

Center *for* Public Service — Portland State UNIVERSITY

TABLE OF CONTENTS

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:

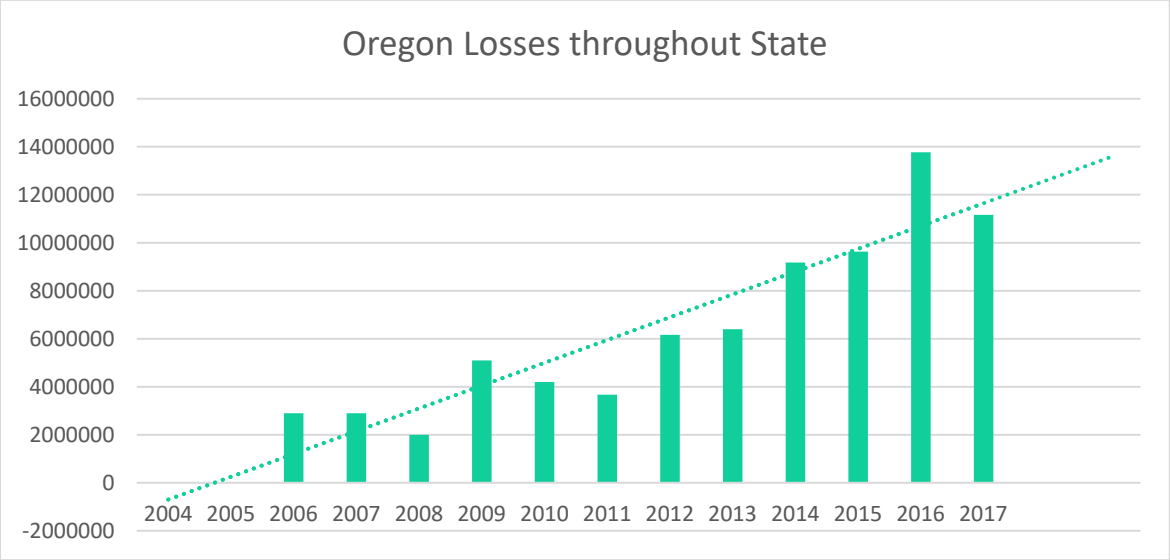
- Losses in 2017 alone: $1.4 Billion[9]
- The average cost of a breach to a small business is between $84,000 and $148,000.[10]
- Time to recover from a breach approximately 50 days
- 43% of breaches affect small companies
- 60% of small businesses close within six months following a breach[11]

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]

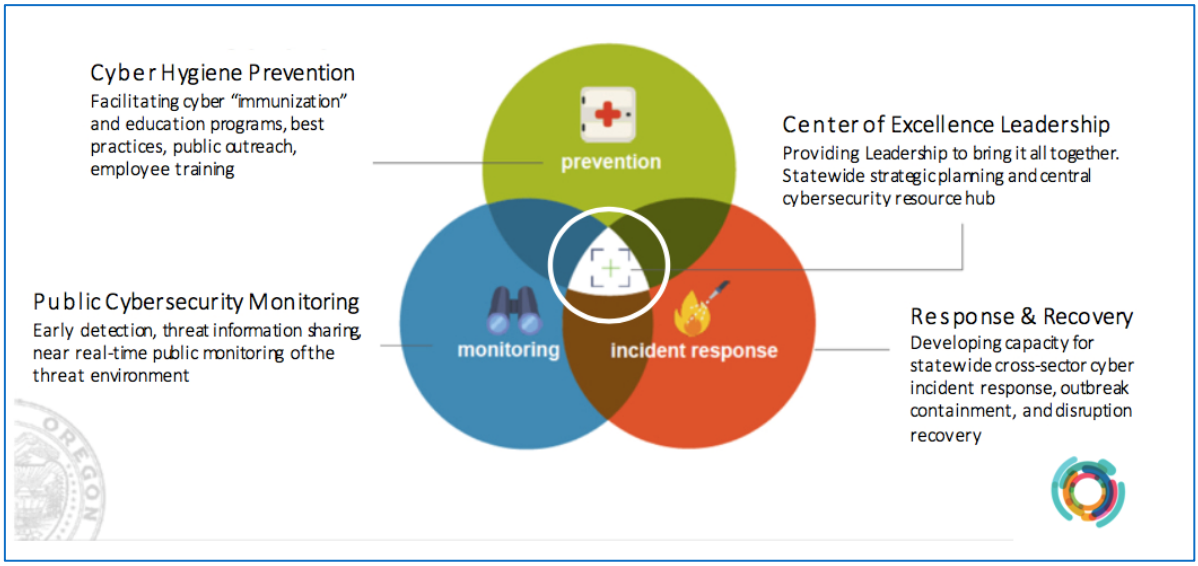


FIGURE 1: CCOE IMPLEMENTATION FRAMEWORK

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.

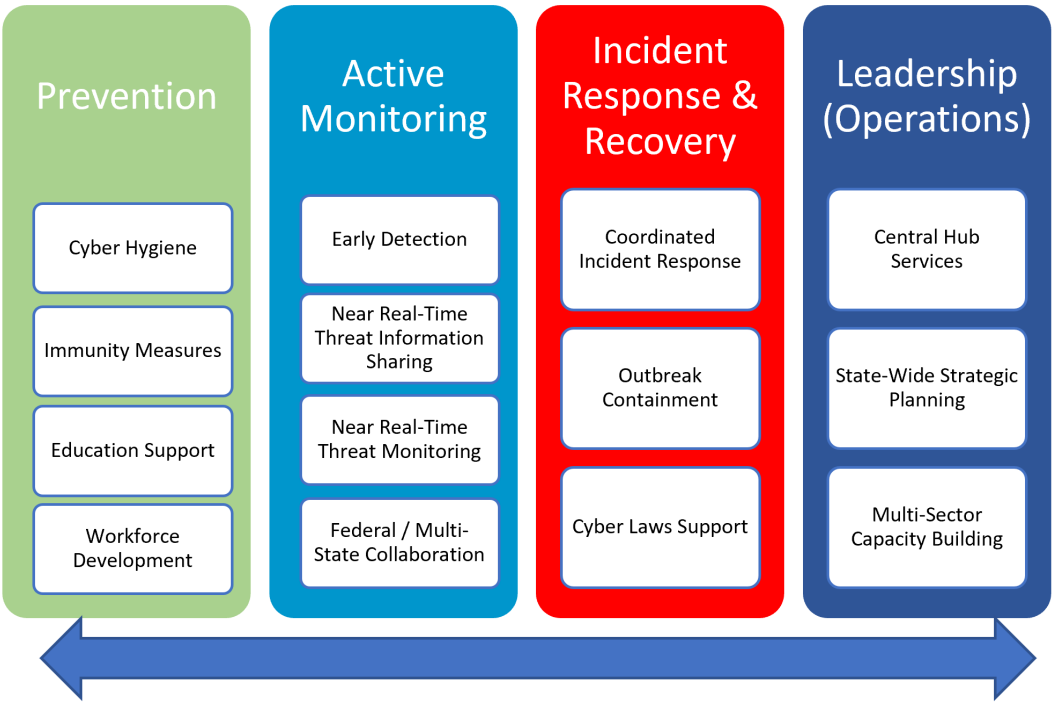


FIGURE 2: CYBERSECURITY ACTIVITY CATEGORIES

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 3[33] 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		
 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	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
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

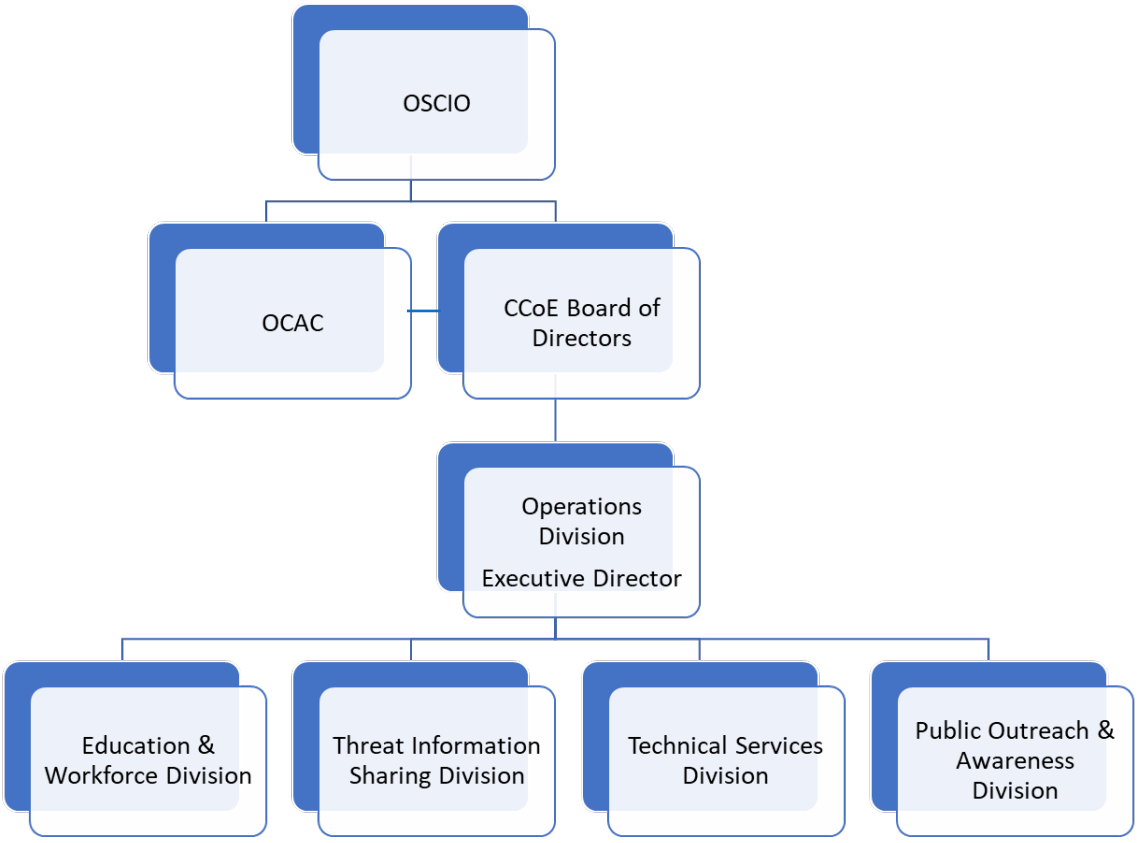


FIGURE 4: PROPOSED ORGANIZATIONAL CHART

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.

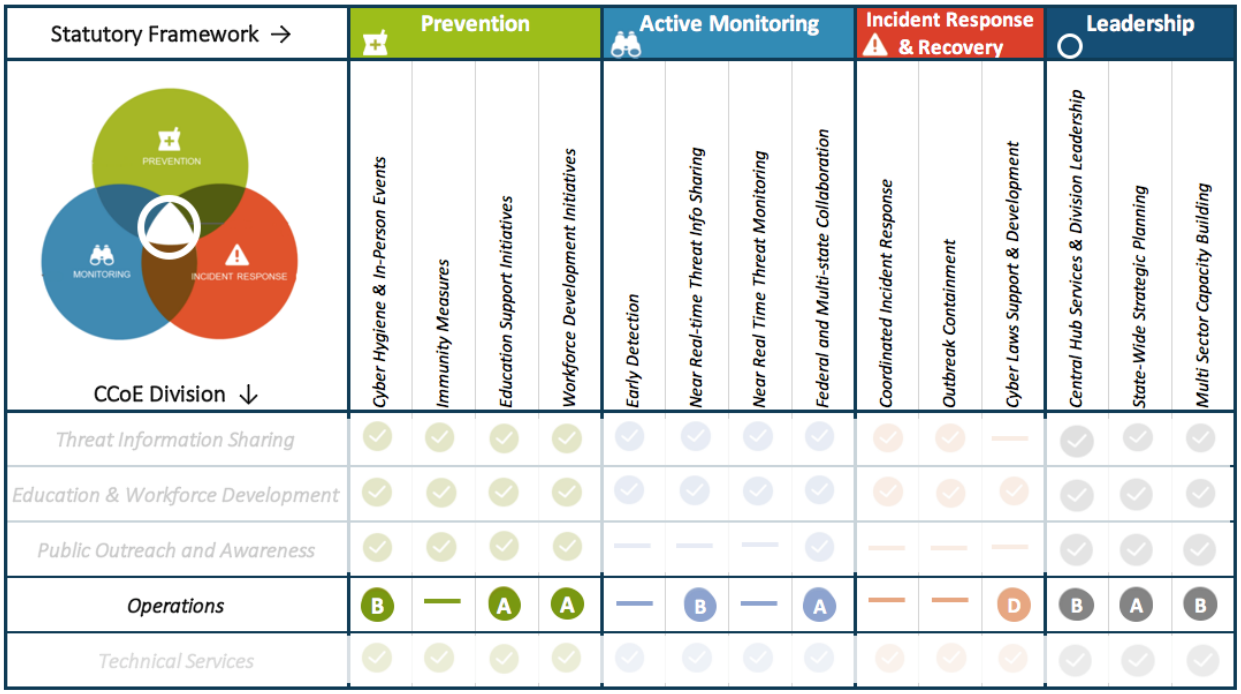


FIGURE 5: STATUTORY REQUIREMENTS - OPERATIONS DIVISION

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 OSCIO[34]

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.

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	D	C	B	B	A	A	A	D	A	A	D	A	C	C
Public Outreach and Awareness	✓	✓	✓	✓	—	—	—	✓	—	—	—	✓	✓	✓
Operations	✓	—	✓	✓	—	✓	—	✓	—	—	✓	✓	✓	✓
Technical Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 6: STATUTORY REQUIREMENTS – EDUCATION AND WORKFORCE DEVELOPMENT DIVISION

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 programs[36]

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.

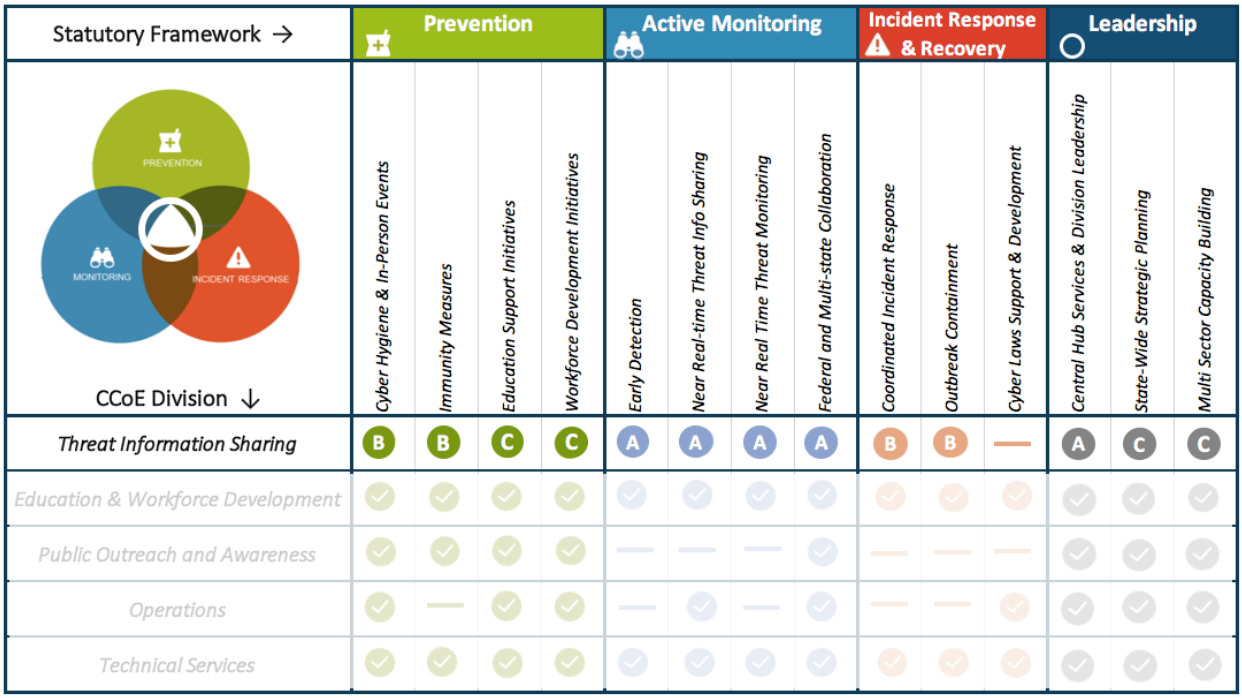


FIGURE 7: STATUTORY REQUIREMENTS - THREAT INFORMATION SHARING DIVISION

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
- National Cybersecurity and Communications Integration Center (NCCIC) and other Department of Homeland Security programs
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Regional and Sector-specific ISAOs (Financial, Health, Social, adjacent states)
- Academic Institutions
- 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.

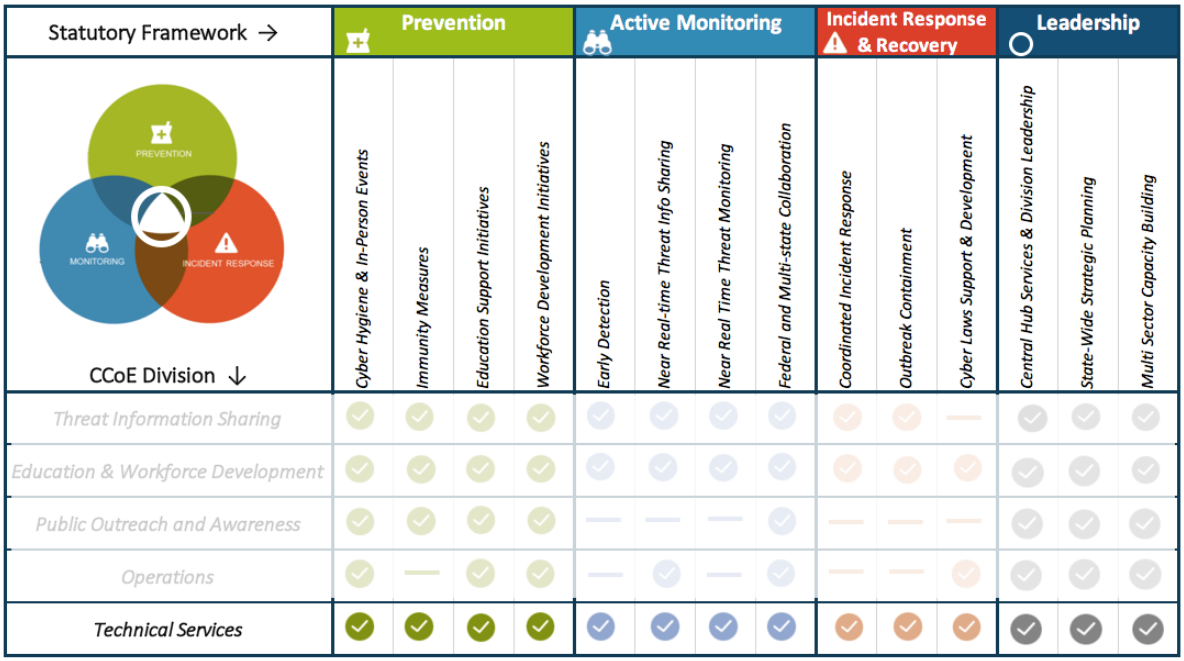


FIGURE 8: STATUTORY REQUIREMENTS - TECHNICAL SERVICES DIVISION

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.

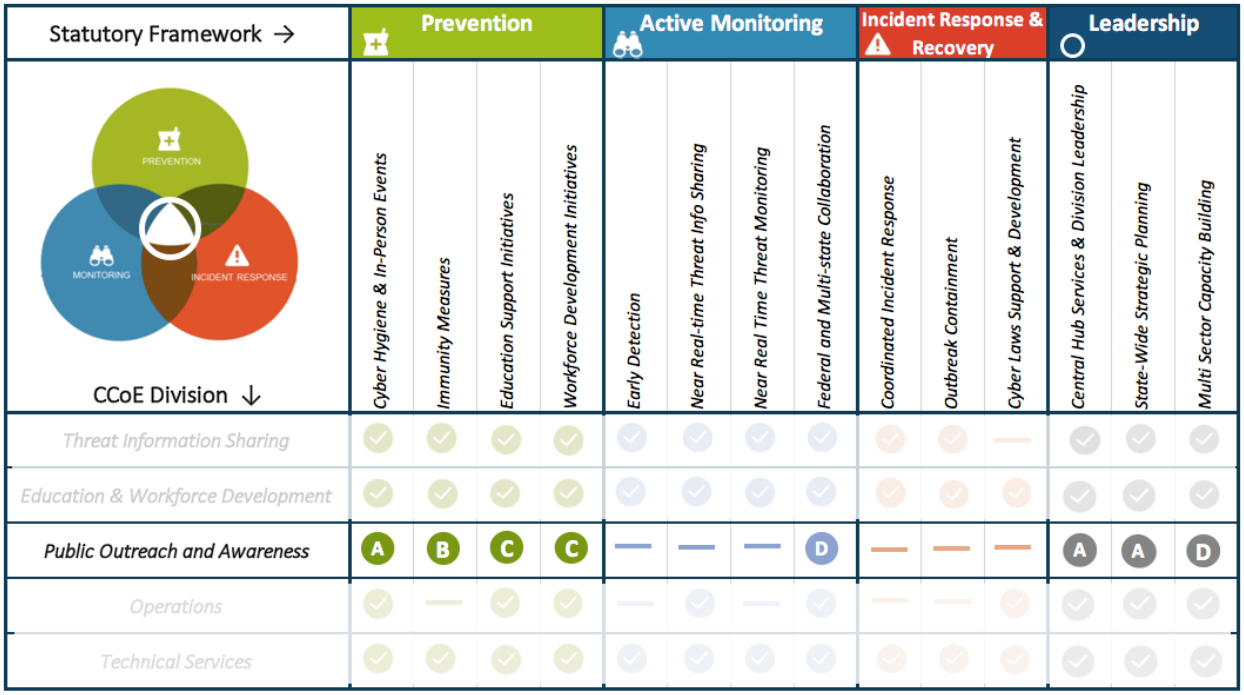


FIGURE 9: STATUTORY REQUIREMENTS - PUBLIC OUTREACH & AWARENESS DIVISION

SB90 Tasks A & B: Prevention and Leadership. Tasks A and B involve coordinating information sharing regarding cybersecurity risks and incidents across all types of organizations[38] 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
- County extension offices
- Small Business Development Centers
- Special districts
- Cybersecurity Industry
- Public agencies, Including State, City, and County, and Tribal leadership
- School districts
- 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

<table>
<tr><td rowspan="2"></td><td colspan="4">Phase I: October 2019-June 2020</td><td colspan="2">Phase II: July 2020-June 2021</td><td>Phase III: July 2021 +</td></tr>
<tr><td>Q1</td><td>Q2</td><td>Q3</td><td>Q4</td><td>H1</td><td>H2</td><td>Y3</td></tr>
<tr><td>Cybersecurity Disruption and Strategic Plan (required biennially)</td><td>Scope plan requirements & identify resources</td><td>Identify plan implementation (contractors / staff)

Begin planning process with state-wide stakeholder engagement</td><td>Continue planning process & engage state-wide stakeholders</td><td>Complete plan</td><td colspan="2">Implement plan</td><td>Evaluate plan and update for biennial submission</td></tr>
<tr><td rowspan="2">Resource Development & Strategic Planning</td><td>Analyze funding resources and collaborative partners for program implementation</td><td>Commence grant writing and other funding source activities</td><td colspan="5">Coordinate and/or oversee program implementation as funding is available</td></tr>
<tr><td colspan="7">Seek additional supporting resources</td></tr>
<tr><td rowspan="2">Division Area Programmatic Plans</td><td>Assess funding availability and program planning</td><td>Engage partners in collaborative actions</td><td colspan="5">Implement programs as partnerships and funding is available</td></tr>
<tr><td colspan="2">Plan evaluation activities to demonstrate public benefit</td><td colspan="2">Monitor programs and collect evaluation data</td><td colspan="3">Evaluate program outcomes*</td></tr>
</table>

*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 Statewide Strategic Planning & Fundraising 10/1/2019 – 6/30/2020	Phase 2 Estimated Program Implementation July 2020 - June 2021	Phase 3 Estimated Program Implementation July 2021 - June 2022	All Phases
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 • K-12 • Higher Educational Institutions **Educational Initiatives** • 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 • OSU OR Security Operations Center (SOC) • Oregon Pathways Project • Oregon Veterans Cybersecurity Initiative	Companion Resource	Operational Partner		Operational Partner	Companion Resource
Private Industry • 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 • 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**
• 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 • 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 Learing
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-cameron
[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.

Cyber Security Center of Excellence Concept Proposal Summaries

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.

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 (OCPP) 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 OCPP 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.

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

Project Name: Statewide Information Sharing and Analysis Organization

Author(s): Dennis Tomlin

Overview: Establishing a statewide Information Sharing and Analysis Organization will allow communities of interest to share cyber threat information with each other on a voluntary basis. The goal is to create deeper and broader networks of information sharing nationally that foster the development

and adoption of automated mechanisms for the sharing of information to elevate the security of the State of Oregon and ultimately, the Nation. Funding for for travel and expenses for attending the National ISAO meeting and other significant workshops or educational opportunities is included.

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.

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.

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.

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.

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 blockchain security. Funding would be required for curriculum development, mentorship, and event organization.

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.

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

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.

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.

OPERATIONS DIVISION PROGRAM MODEL FOR CCOE

Inputs		Outputs		Outcomes
Resources	Possible Partners	Activities	Target Audience	Expected Change
1. Legal Framework 2. State Funds – Legislative 3. Grants from private, academic, scientific, educational, and defense institutions 4. Oregon Cybersecurity Advisory Council 5. OSCIO 6. CCoE Membership fee based services	1. PSU, OSU, OHSU, Lewis & Clark College, OU, and other institutions of higher ed 2. Business and Industry Partners 3. Information security stakeholders	1. Coordinate and align data and information among partners 2. Complete CCoE operational business plan 3. Complete Oregon Cybersecurity Strategy 4. Complete Cyber Disruption Response Plan 5. Generate resources with CCoE and other partners 6. Coordinate and manage budget, revenues, and fees for CCoE 7. Engage with high-level stakeholder, partner, beneficiary, and funding opportunities 8. Develop and disseminate best practices in procurement, policy, and legal issues 9. Oversight for program area plans and implementation	1. Executive and legislative level administrators in state, local, and tribal government agencies 2. Executive level Law enforcement agencies, DOJ, Oregon AG, FBI, Dept of Homeland Security etc. 3. Executive Level administrators in Medical, Legal, Private Sectors and Non-Profit Sector organizations 4. State-level Executives in Economic Development, Commerce, Department of Consumer & Business Services, and Education (K-20) including private Education Executives and CTOs 5. Oregon Cybersecurity Advisory Council 6. OSCIO 7. Oregonians and those affected by strategic planning implementation	1. Increased resilience to cyber threats across Oregon 2. Increased coordination among a wide network of engaged organizations 3. Increased awareness of cybersecurity 4. Increased visibility of and participation in Oregon's community-based cybersecurity expertise and preparedness 5. Lessened risk of breach 6. Reduced cost of recovery

EDUCATION AND WORKFORCE DIVISION PROGRAM MODEL

Inputs →		Outputs →		Outcomes
RESOURCES	POSSIBLE PARTNERS AND COLLABORATORS	ACTIVITIES	TARGET AUDIENCE	EXPECTED CHANGE
1. State Funding 2. Potential Partnerships 3. Membership and fee based services 4. Students 5. Veterans 6. Cybersecurity Professionals 7. Cybersecurity Industry	1. Higher education institutions (MHCC, OSU, OregonTech, PSU, UO, OHSU, PCC, RCC, LCC, SOU etc.) 2. Oregon Fiber Partnership 3. OR TITAN fusion center collaboration 4. Cybersecurity Industry 5. Computer Science Industry 6. ISAO Network from Threat Division 7. DHS/FBI/DOJ/State Police 8. Critical Infrastructure Owner/Operators 9. Academic Institutions (K-12) 10. National Guard 11. Oregon Veterans Cybersecurity Initiative 12. NW Cyber Camps 13. OSU ORTSOC team 14. The State of Oregon 15. Oregon Cyber Pathways Project	1.Teaching SOC - Cyber incident and response management 2. Veterans SWAT team 3. Educational competition support and promotion 4. Structured Mentor Program 5. Internships 7. Participation in Strategic and Cyber Incident Disruption and Response planning 8. Support Cybersecurity research 9. Encourage multi-sector industry investment and partnership with post-secondary institutions of education and other career readiness programs 10. Developing K-12 student and teacher computer science capacity and literacy building tools and partnerships	1. State, Local, and Tribal government organizations 2. Elementary and secondary educational institutions K-12 3. Higher Ed 4. Small to medium sized businesses of all kinds, but specifically: Financial, Legal, Health, and high value targets 5. Rural Organizations 6. Non-Profit organizations 7. Other Protectors of Personally Identifying Information, Protected Health Information, Payment Card Industry data[4] 8. Computer Science Students 9. Veterans in need of workforce retraining 10. Civilians in need of workforce retraining	1. Increased State-Wide access to response and recovery assistance for cyber disruptions. 2. Increased access to immediate threat information, and best practices 3. Centralized cyber emergency response system for Oregonians[5] 4. Increased educational opportunities in the cybersecurity field 5. Increased numbers of qualified cybersecurity professionals 6. Increased cyber literacy in K-12 students 7. Increased connection to workforce pathways for Oregon students 8. Increased Veteran participation in the cybersecurity workforce 9. Increased state employee cyber security awareness and capacity

[4] Target audience(s) #1-7 include recipients of SOC services – overlap with ISAO / Tech Services

[5] Outcomes #1-3 are related to SOC services – overlap with ISAO / Tech Services

CCoE Information Sharing Program Model

Inputs →		Outputs →		Outcomes
RESOURCES	Possible Partners and Collaborators	Activities	Target Audience	Expected Change
1. State Funding 2. Potential Partnerships with shared resource partnerships 3. Membership and fee based services	1. OR Titan Fusion Center 2. National Cybersecurity and Communications Integration 3. Multi-State Information Sharing and Analysis Center 4. Regional and Sector-specific ISAOs (Financial, Health, Social, adjacent states) 5. Academic Institutions 6. Dept. Homeland Security 7. FBI 8. DOJ 9. Oregon Fiber Partnership 10. BSIDES	1. Maintain and monitor consensus-based standards development process: contractual agreements including non-disclosure and non-attribution agreements, business processes, operating procedures, technical specifications, and privacy protections. 2. Face-to Face engagement state-wide through Cyber summits, Breakfast, luncheon, and town hall type events, especially in rural areas 3. Draft internal CCoE Information Sharing and Analysis Organization Plan proposal 4. ISAO implementation 5. Information Sharing division involvement in State-wide Strategic Planning	1. State, Local, and Tribal government organizations 2. Elementary and secondary educational institutions 3. Higher – Ed 4. Small to medium sized businesses of all kinds, specifically: Financial, Legal, Health, and high value targets 5. Rural Organizations 6. Non-Profit organizations 7. Members of the public 8. Other Protectors of Personally Identifying Information, Protected Health Information, Payment Card Industry data, Protected Critical Infrastructure Information (classified) 9. Critical Infrastructure Owner/Operators	1. Increased threat specific state-wide situational awareness 2. Increased awareness and visibility of preventative cybersecurity culture. 3. Increased access to immediate threat information, best practices, and opportunities for face-to-face engagement 4. Trustworthy and transparent centralized information sharing system for Oregonians based on consensus driven standards and focused on mutual trust and privacy. 5. Increased public value accumulated through securing systems and mitigating costly attacks. 6. Public Value added through increased access to affordable cybersecurity options to underserved Oregonians.

CCoE Technical Services Program Model

Inputs →		Outputs →		Outcomes
Resources	Possible Partners	Activities	Target Audience	Expected Change
1. Advanced students 2. Faculty 3. Industry professionals 4. Capital (e.g., hardware) 5. Operational funds (software, cloud services, connectivity) 6. Facilities 7. Membership and fee-based services	1. Academic Institutions (K-12) 2. Higher education institutions (MHCC, OSU, OregonTech, PSU, UO, OHSU, OR Fusion IT Center, PCC, RCC, LCC, SOU) 3. Oregon Fiber Partnership 4. OR TITAN Fusion Center collaboration 5. Cybersecurity Industry	1. Operate central call center 2. Develop cybersecurity controls 3. Provide managed security services 4. Manage internships to promote workforce training and service delivery 5. Provide Triage Teams 6. Offer referrals to advanced resources, law enforcement, or other resources 7. Manage Emergency Incident Response 8. Customer acquisition: Reach and educate those who may lack cybersecurity awareness 9. Assist target audience with resources to develop cyber security disruption plans 10. Assist in State-wide Cyber Disruption and Response Plan and Cybersecurity Strategic Planning 11. Technical and IT Services for all CCoE Divisions	1. Underserved organizations that can't afford commercial prices and are currently under protected (e.g., public schools; small businesses, farms). 2. Protectors of Personally Identifying Information, Protected Health Information, Payment Card Industry data, Protected Critical Infrastructure Information (classified) 3. Geographically diverse distribution focusing on rural and underserved in metropolitan counties 4. Small to medium sized businesses of all kinds, but specifically: Financial, Legal, Health, and high value non-profit sector targets 5. Farms, minority owned, women owned and veteran owned businesses	1. Increase basic measures of protection in small and underserved organizations 2. Reduced losses due to cybercrime 3. Reduce number of cyber incidents in the state 4. Reduction in time from data breach to detection and containment 5. Increased capacity for small organizations to respond to and mitigate cyber crime 6. Increase in services in Oregon that are within reasonable driving distance (2 hours) from all locations 7. Increase in security of Oregon's networks and increasing herd immunity

CCoE Public Awareness & Outreach Program Model

Inputs		Outputs		Outcomes
Resources	Possible Partners	Activities	Target Audience	Expected Change
1. State Funds 2. Conference sponsors 3. Other engagement sponsors	1. Rural area regional chambers of commerce, county extension offices, Small Business Development Center channels 2. Cybersecurity Industry 3. Public agencies	1. Event Marketing: Multi-sector (vertical) events and conferences monthly and yearly events throughout the state. 2. Assist CCoE Divisions to market programs and events 3. Promote workforce development and create awareness of career opportunities 4. Promote legislative initiatives 5. Provide access to information tools to help Oregon businesses and organizations improve cybersecurity 6. Cybersecurity expert Speaker placement program 7. Lessons, resource, stories, and expertise sharing through communications channels such as newsletters, social media and earned media (news articles) and paid media (advertising, promotion) throughout the state 8. Strategic marketing campaigns and programs 9. Public awareness building programs involving the use of social media, traditional print media, online media, electronic media and outdoor media 10. Annual (or potentially bi-annual) audience perception/awareness survey. 11. Conduct research about how to improve the program's effectiveness evaluation metrics on increased cybersecurity awareness, including impressions, website traffic, number of social media followers and level of engagement, event attendance, and search rankings 12. Provide opportunities for training	1. Small businesses 2. School districts 3. State agencies, state, local, and tribal government agencies 4. Law enforcement agencies 5. Financial Services 6. Medical 7. Legal 8. Non-Profit Sector 9. Individual 10. Parents & Children	1. Increased awareness across Oregon for cybersecurity business and educational programs, workforce availability, and companies 2. Increased visibility of cybersecurity threats and opportunities for cyber hygiene 3. Increased access to cybersecurity experts, cybersecurity education, and hands-on training

Appendix B: Cyber Disruption Plan Required Elements

Cyber Disruption and Response Plan Tasks Required by ORS276A.326-29

1) Detail the steps Oregon should take to increase the resiliency of its operations in preparation for, and during the response to, a cyber disruption event
2) Address high-risk cybersecurity for the state's critical infrastructure, including a review of information security technologies currently in place to determine if current policies are sufficient to prevent the compromise or unauthorized disclosure of critical or sensitive government information inside and outside the firewall of state agencies, and develop plans to better identify, protect from, detect, respond to and recover from significant cyber threats
3) Establish a process to regularly conduct risk-based assessments of the cybersecurity risk profile, including infrastructure and activities within this state;
4) Provide recommendations related to securing networks, systems and data, including interoperability, standardized plans and procedures, evolving threats and best practices to prevent the unauthorized access, theft, alteration or destruction of data held by the state;.
5) Include the recommended content and timelines for conducting cybersecurity awareness training for state agencies and the dissemination of educational materials to the public and private sectors in this state through the center
6) Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information
7) Include strategies for collaboration with the private sector and educational institutions through the center and other venues to identify and implement cybersecurity best practices
8) Establish data breach reporting and notification requirements in coordination with the Department of Consumer and Business Services.

Appendix C:
Funding Sources for Cybersecurity :
Federal and Foundation Grants

Federal Grants

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	CyberCorps Scholarships for Service (SFS) Provides funding to award scholarships to students in cybersecurity. All scholarship recipients must work after graduation for a Federal, State, Local, or Tribal Government organization in a position related to cybersecurity for a period equal to the length of the scholarship. (A proposing institution must provide clearly documented evidence of a strong existing academic program in cybersecurity (e.g., CAE certification)	Education and Workforce Development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991	February 4, 2019 July 31, 2019 July 31, 2020	*Supports* up to three years of stipends, tuition and allowances for students in the general area of cybersecurity. A typical award might be approximately $3-5 million for five years supporting four cohort classes of six students each. Total award sizes will depend upon the tuition amount and on the cost of management and development. *Capacity Track* projects were eliminated in last cycle. *Lewis and Clark College previously awarded two capacity grants: - development of tools that automatically assess student learning in practical cybersecurity tasks (joint grant) -EDURange: facilitating teaching of cybersecurity (joint grant) No Oregon institutions funded for scholarships	*Institutions of Higher Education (IHEs) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Community colleges are eligible only as either non-lead collaborating institutions or sub-awardees of the partnering four-year SFS institutions*

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Campus Cyberinfrastructure (CC*) The Campus Cyberinfrastructure (CC*) program invests in coordinated campus-level networking and cyberinfrastructure improvements, innovation, integration, and engineering for science applications and distributed research projects. Learning and workforce development (LWD) in cyberinfrastructure is explicitly addressed in the program. Science-driven requirements are the primary motivation for any proposed activity.	Education and Workforce development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504748	February 20, 2019	Approximately $10 million-$17 million will be made available in FY 2018 to support 13-26 awards, subject to the availability of funds. *Portland State University awarded $500,000 in 2015 for network infrastructure upgrades with associated research opportunities for minorities and underrepresented groups in the STEM disciplines	U.S.-based universities and two and four-year colleges nonprofit nonacademic institutions

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Innovative Technology Experiences for Students and Teachers (ITEST) Successful ITEST projects will engage students in research studies that: (1) promote student awareness of, interests in, and capacities to participate in STEM occupations or education pathways leading to those occupations; and (2) advance knowledge of promising interventions and the conditions and contexts that influence their success in promoting STEM career awareness among PreK-12 students. ITEST projects may engage students in school or out of school, or through a blend of learning environments. Projects that examine the effectiveness of engaging adult volunteers with relevant disciplinary expertise from academia or industry to mentor or engage students are encouraged, as are projects that would engage students in the uses of cutting-edge technologies, in computing or computational thinking, or in work or problem based experiences involving their use.	Education and Workforce Development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5467	August 14, 2019 Second Wednesday in August, Annually Thereafter	2-4 Exploratory awards with durations up to two years and total budgets up to $400,000 each 6-12 Strategies awards with durations up to three years and total budgets up to $1,200,000 each 1-2 SPrEaD (Successful Project Expansion and Dissemination) awards with durations of three to five years and total budgets up to $2,000,000 each. *Oregon State University awarded $156,903.00 in 2017 for project targeting rural women age 15-18 with no prior interest in science for experiences to skills and career pathways in information and communication technology More information: infrastructure upgrades https://www.nsf.gov/awardsearch/showAward?AWD_ID=1657217&HistoricalAwards=false	Open to all NSF categories of proposers

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Training-based Workforce Development for Advanced Cyberinfrastructure (CyberTraining) This program seeks to prepare, nurture, and grow the national scientific research workforce for creating, utilizing, and supporting advanced cyberinfrastructure (CI) to enable and potentially transform fundamental science and engineering research and contribute to the Nation's overall economic competitiveness and security.	Workforce development, best practices	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505342	February 06, 2019 January 15, 2020 Third Wednesday in January, Annually Thereafter	Pilot Projects: up to $300,000 total budget with durations up to two years; Implementation Projects: Small (with total budgets of up to $500,000) or Medium (with total budgets of up to $1,000,000) for durations of up to four years; and Large-scale Project Conceptualization Projects: up to $500,000 total budgets with durations up to 2 years.	Open to all NSF categories of proposers

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Office of Advanced Cyberinfrastructure: Research Core Program The Office of Advanced Cyberinfrastructure (OAC) supports translational research and education activities in all aspects of advanced cyberinfrastructure (CI) that lead to deployable, scalable, and sustainable systems capable of transforming science and engineering research.	Best practices Technical Services Multi-disciplinary, extreme-scale, driven by science and engineering research, end-to-end, and deployable as robust research CI	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505571	October 31, 2019 - November 14, 2019	Small Projects - up to $500,000 total budget with durations up to three years.	Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Secure and Trustworthy Cyberspace (SaTC) The goals of the SaTC program are aligned with the Federal Cybersecurity Research and Development Strategic Plan (RDSP) and the National Privacy Research Strategy (NPRS) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. The RDSP identified six areas critical to successful cybersecurity research and development: (1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure. • CORE: Main focus of the SaTC research program: Computer and Information Science and Engineering (CISE), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral and Economic Sciences (SBE). • EDU: The Education (EDU): Proposals focusing entirely on cybersecurity education. • TTP: The Transition to Practice (TTP) designation: Proposals that are focused exclusively on transitioning existing research results to practice.	Education and Workforce Development Technical Services Administration and Policy	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709	Full Proposal Accepted Anytime	CORE and TTP proposals may be submitted in one of the following project size classes: • Small projects: up to $500,000 in total budget, with durations of up to three years; • Medium projects: $500,001 to $1,200,000 in total budget, with durations of up to four years; EDU proposals are limited to $500,000 in total budget, with durations of up to three years.	Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
National Science Foundation	Advanced Technological Education (ATE) The ATE program supports curriculum development; professional development of college faculty and secondary school teachers; career pathways; and other activities. The program invites research proposals that advance the knowledge base related to technician education. It is expected that projects be faculty driven and that courses and programs are credit bearing although materials developed may also be used for incumbent worker education. The ATE program focuses on colleges that award two-year degrees in advanced technology fields and expects these colleges and their faculty to have significant leadership roles on all projects. Effective technological education programs should involve partnerships in which two-year institutions work with four-year institutions, secondary schools, business, industry, economic development agencies, and government."	Workforce development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5464	October 03, 2019 October 01, 2020	45 to 75 awards, total awarded $59,000,000 – individual budgets vary depending on designation as Projects, Centers, or Targeted Research on Technician Education. *Klamath Community College awarded $199,986.00 for a rural virtual internship program for STEM fields. More info here: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1601075&HistoricalAwards=false *Notably, this is also a major funding source ($2,202,387.00 in 2015) for CyberWatchWest consortium out of Whatcom Community College (Bellingham, WA).	Open to all NSF categories of proposers – focused on programs at community colleges and minority servcing institutions
National Science Foundation	Cybersecurity Innovation for Cyberinfrastructure (CICI) Cybersecurity Innovation for Cyberinfrastructure (CICI). CICI seeks three categories of projects: Secure Scientific	CCoE	https://www.nsf.gov/publications/pub_summ.jsp?WT.z_pims_id=505159&ods_key=nsf19514 https://www.nsf.g	January 23, 2019	No Oregon funding.	Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
	Cyberinfrastructure (SSC): Secure the scientific workflow by encouraging novel and trustworthy architectural and design approaches, models and frameworks for the creation of a holistic, integrated security environment that spans the entire scientific CI ecosystem. Includes the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems Program. Research Data Protection (RDP): Provide solutions that ensure the provenance of research data and reduce the complexity of protecting research data sets regardless of funding source. Cybersecurity Center of Excellence (CCoE): This award seeks to provide the NSF community with a centralized resource of expertise and leadership in trustworthy cyberinfrastructure.		ov/funding/pgm_summ.jsp?pims_id=504996			their faculty members. Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.
National Science Foundation	Community College Cyber Pilot Program "Community College Cyber Pilot (C3P) program as part of NSF's CyberCorps®: Scholarship for Service (SFS) program. Specifically, NDAA18 **authorizes scholarships** for	Education and Workforce Development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505573	July 2018 (rolling thereafter)	Collaborative Research: Modeling Student Activity and Learning on Cybersecurity Testbeds Award Number:1723714; Principal Investigator:Jens Mache; Co-Principal Investigator:; Organization:Lewis and Clark College;NSF Organization:DGE Start Date:09/01/2017; Award	Community Colleges

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
	eligible students who: are pursuing associate degrees or specialized program certifications in the field of cybersecurity; and (A) have bachelor's degrees or (B) are veterans of the Armed Forces"				Amount:$124,965.00; EDURange: Supporting cyber security education with hands-on exercises, a student-staffed help-desk, and webinars Award Number:1516100; Principal Investigator:Jens Mache; Co-Principal Investigator:; Organization:Lewis and Clark College;NSF Organization:DGE Start Date:08/01/2015; Award Amount:$166,526.00;	
NSF Division of Electrical, Communications and Cyber Systems	The Energy, Power, Control, and Networks (EPCN) Program supports innovative research in modeling, optimization, learning, adaptation, and control of networked multi-agent systems, higher-level decision making, and dynamic resource allocation, as well as risk management in the presence of uncertainty, sub-system failures, and stochastic disturbances. EPCN also invests in novel machine learning algorithms and analysis, adaptive dynamic programming, brain-like networked architectures performing real-time learning, and neuromorphic engineering. EPCN's goal is to encourage research on emerging technologies and applications including energy, transportation, robotics, and	Technical Services Education and Workforce Development Information Sharing	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505249	Full proposals accepted anytime	Oregon State University award of $410,000. September 2017-August 2010. Portland State University award for $360,000. August 2018-July 2021.	Institutions of Higher Education Nonprofit Organizations For-Profit Organizations State and Local Governments Unaffiliated Individuals Foreign Organizations Other Federal Agencies

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
	biomedical devices & systems. EPCN also emphasizes electric power systems, including generation, transmission, storage, and integration of renewable energy sources into the grid; power electronics and drives; battery management systems; hybrid and electric vehicles; and understanding of the interplay of power systems with associated regulatory & economic structures and with consumer behavior. Areas managed by program directors • Control Systems • Energy and Power Systems • Power Electronics Systems • Learning and Adaptive Systems					
National Science Foundation Computer Science for All. Researcher Practitioner Partnerships (CSforAll:RPP)	This program aims to provide all U.S. students the opportunity to participate in computer science (CS) and computational thinking (CT) education in their schools at the preK-12 levels. With this solicitation, the National Science Foundation (NSF) focuses on researcher-practitioner partnerships (RPPs) that foster the research and development needed to bring CS and CT to all schools. Specifically, this solicitation	Education and Workforce Development	https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505359	February 12, 2019 Second Tuesday in February, Annually Thereafter	Related programs funded. Appears to be a new program. Estimated Number of Awards: 24 approximately 10 small, 11 medium, and 3 large awards. Anticipated Funding Amount: $20,000,000	The categories of proposers eligible to submit proposals to the National Science Foundation are identified in the NSF Proposal & Award Policies & Procedures Guide (PAPPG), Chapter I.E.

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
	aims to provide high school teachers with the preparation, professional development (PD) and ongoing support that they need to teach rigorous computer science courses; preK-8 teachers with the instructional materials and preparation they need to integrate CS and CT into their teaching; and schools and districts the resources needed to define and evaluate multi-grade pathways in CS and CT.					
Department of Agriculture – Rural Development	Rural Business Development Grants Enterprise grants must benefit rural areas or towns outside of urbanized periphery of cities with populations of 50,000 or more. Grants can be used for a variety of purposes; most relevant for CCoE and SB90 are adult distance learning and technology-based economic development. Opportunity grants can be used for technology-based economic development and, more generally, community economic development.	Workforce development; Incident response and investigation capabilities CCoE Policy and Administration	https://www.rd.usda.gov/programs-services/rural-business-development-grants	Vary by state; must contact Oregon program officials for current application procedures	Grants typically range from $10,000 to $500,000, with smaller grants given higher priority.	Rural public entities including, but not limited to: Towns Communities State agencies Authorities Nonprofit corporations Institutions of higher education Federally-recognized Tribes Rural cooperatives (If organized as a private nonprofit corporation)

Funding Entity	Funding Opportunity Description	Alignment with SB90	Source	Application window	Funding range / Oregon Funding	Proposer specifications
Department of Homeland Security	FY 2017 Nonprofit Security Grant Program (NSGP) Provides funding for building and sustaining core capabilities and strengthening multi-sector governance integration, including through "target hardening" via cybersecurity, and cybersecurity training for nonprofit staff.	Information Sharing Technical Services	https://www.fema.gov/media-library-data/1526585999645-b157aa32e8dda49c604e82c6202b6d7e/FY_2018_NSGP_NOFO_051718_508.pdf	Appears to be rolling deadline in Spring of each year	Up to $150,000	Must be 501(c)(3) nonprofit organization

Foundation Grants

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
Esco Foundation	Limited information online. Contact foundation for details on funding technology and education. Recently funded $25,000 for makerspace at University of Portland engineering school	Potentially all	No website P.O. Box 3121, Portland, OR United States 97208-3121 Telephone: (503) 225-2935	Telephone: (503) 225-2935	Not available
Verizon	STEM learning	Workforce development	http://www.verizon.com/about/responsibility/giving-and-grants	Small – most around $1,000	Must be 501c(3)
PacifiCorp Foundation	Educational and research organizations both public and private, from early childhood through university level (proposals due March 15) Environment, civic and community enhancement and other organizations not covered in other categories (due June 15)	Workforce development	https://www.pacificpower.net/about/itc/foundation/afg/er.html	Grants generally are less than $10,000 with most between $2,000 and $5,000) ;	Must be 501c(3)

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
BestBuy Foundation	Best Buy Foundation is searching for local organizations with a demonstrated track record for building skill proficiency in technology through out-of-school time programs. Programs should help teens build tech skills by utilizing cutting-edge technology such as computers, digital cameras, video cameras and professional software in a wide range of areas including: Coding or programming Computer maintenance and repair Maker Faires/hack-a-thons	Education and Workforce Development	https://corporate.bestbuy.com/community-grants-page/	Grants average $5,000; will not exceed $10k	Eligible nonprofits may be a public or nonprofit community-based organization (e.g., community center, school or library) with existing local or regional out-of-school time program and a proven track record of serving youth ages 13-18; 25 miles from a Best Buy store, commitment to diversity and inclusion.
Braemer Charitable Trust	Actively seeks grant applications with emphasis on Education, Community Service, Cultural, Youth Activities and Historical Preservation with funding to $10,000. Grant applications for specific projects that will be completed in one year, have project budgets less than $50,000 and contain an educational factor viewed more favorably.	Workforce development (especially youth)	No website. Trust Management Services, LLC PO Box 1990 Waldport OR 97394 Phone: 541 563-7279 Fax: 541 563-7216 Melissa Reimers EMail: Info@trustmanagementservices.net	Not in excess of 10,000	Tax-exempt organizations in Oregon. No individuals. Project budgets below $50,000.

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
American Honda Foundation	Grant making that reflects the basic tenets, beliefs and philosophies of Honda companies, which are characterized by the following qualities: imaginative, creative, youthful, forward-thinking, scientific, humanistic and innovative. We support youth education with a specific focus on the STEM (science, technology, engineering and mathematics) subjects in addition to the environment.	Education and Workforce Development (Youth priority)	https://www.honda.com/community/applying-for-a-grant	The grant range is from $20,000 to $75,000 over a one-year period.	Nonprofit charitable organizations classified as a 501(c) (3), or a public school district, private/public elementary and secondary Schools. Gross revenue under $500,000.
Hoover Family Foundation	Priorities of Interest Programs that foster self-sufficiency Effective providing of social services Improvement of educational opportunities at all levels Programs that aid low-income individuals	Workforce development	http://hooverff.org/	Completed proposals must be received by or postmarked by the following dates: July 1, November 1 or March 1	Funds organizations that provide services within Portland Metro Urban Growth Boundary

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
Oregon Community Foundation	Howard Vollum American Indian Scholarship For Native American residents of Clackamas, Multnomah or Washington counties in Oregon or Clark County in Washington, who are seeking a post-secondary degree in science, computer science, engineering or math. Verl and Dorothy Miller Native American Vocational Scholarship For Native American residents of Oregon who are seeking vocational training or certification. Darlene Hooley Scholarship for Oregon Veterans For Oregon National Guard and Oregon Reservists who have served or been deployed overseas in the post-9/11 conflict, also known as the Global War on Terror.	Education and Workforce Development	https://www.oregoncf.org/grants-scholarships/scholarships	March 1 for following year	Individuals - Students

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
Meyer Memorial Trust	Capacity, project grants, and operating support. All proposals must advance one of the following funding goals: • Build a movement to align community + education institutions to create systems- and policy-level impact • Improve student achievement and college and career readiness	Workforce Development	https://mmt.org/education	Funding deadline(s) approximately early Spring	Not available

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
PGE Foundation	Direct resources to programs preparing young people to be future ready, including supporting hands-on applied learning experiences that develop essential skills, provide adult mentorship or collective impact models that support system-wide transformation. Of particular interest are projects, programs or organizations that transform teaching methods that connect students to goals and aspirations, that measure age-appropriate development of essential skills (aka socio-emotional skills.) Priority will go to projects, programs or organizations that provide evidence that communities served were included in the development of the projects and/or programs and that can provide examples of intentionally focusing on communities that have faced historic or systemic barriers to reaching equal outcomes.	Workforce development	http://www.pgefoundation.org/how_we_fund.html	Nov. 26, 2018 – Jan. 11, 2019 for March decision	Must be 501c(3)

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
US Bank Foundation	Workforce Education and Economic Prosperity and Investing in the Workforce programs. Support programs and organizations that help small businesses thrive, allow people to succeed in the workforce, provide pathways to higher education, and gain greater financial literacy.	Education and Workforce Development	https://www.usbank.com/community/community-possible-grant-program-work.aspx	Most common grant $5,000 Applications open April 1-30	Must be 501c(3)
Intel Foundation	The Intel Foundation encourages multi-sector partnerships that deploy innovative programs that ensures the next generation of innovators is more diverse by gender, race, ethnicity, geography, ability, and social class. Offers matching grants, intel employee volunteer hours, and employee service corps	Education and Workforce Development	https://www.intel.com/content/www/us/en/corporate-responsibility/intel-foundation-funding.html	Rolling. Does not accept unsolicited proposals.	Not available
Jackson Foundation	Broadly funds projects of interest to the City of Portland or statewide interest	Workforce development	http://www.thejacksonfoundation.com/js/rules	Average Amount Grant Rewarded: $ 3,370 Largest Grant Awarded: 50,000 Smallest Grant Awarded: 1,000 Funds awarded quarterly	Tax-exempt organizations

Funding Entity	Funding Opportunity/ Funder interests	SB 90 Alignment	Website or other contact information	Funding Range and Application Window	IRS/ Nonprofit specifications
Harvest Foundation	Grants awarded for community social service agencies that promote economic self-sufficiency through education and training of youth or families with children. And for educational organizations to fund technology training for teachers and technology curriculum development	Education and Workforce Development	http://www.harvestf.org/grantguidelines.htm#EducationGuidelines	The Foundation awards annual grants in the amount of $10,000 each. Multi-year grants are not considered. Grants will not be made to the same organization for more than three consecutive years.	Must be 501c(3)
KeyBank Foundation	KeyBank Foundation, a nonprofit charitable foundation funded by KeyCorp, supports organizations and programs that aim to prepare individuals for successful futures. As a corporate neighbor, our mission is advanced through our three funding priorities: Neighbors, Education, and Workforce, and assisted by our employees' community service efforts.	Workforce development	https://www.key.com/about/community/community-partners.jsp 1211 SW Fifth Avenue, Suite 300 Portland, OR 97204 253-305-7440 KeyBank_Foundation@keybank.com	n/a	Not available