Cybersecurity Services, Education, and Funding: Best Practices and Strategy for Capacity Building in Oregon

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*
Francisco Marin, Ph.D Candidate – *Policy Analyst*

Center *for* Public Service

Portland State
UNIVERSITY

Contents

Executive Summary

This report, *Cybersecurity Services, Education, and Funding: Best Practices and Strategy for Capacity Building in Oregon*, builds on the ongoing efforts to increase the cybersecurity posture in the state of Oregon. This report was a limited scope project funded as part of a larger contract between the Office of the State Chief Information Officer and Portland State University's Center for Public Service.

The goal for this report was to better understand how to both meet the needs of organizations in the state while advancing workforce development and funding support. If successfully achieved, each could significantly increase the cybersecurity posture in state.

This report is developed in three sections, including a) identifying best practices to increase security services for underserved organizations; b) identifying workforce development and experiential educational opportunities and best practices; and c) considerations for increasing funding support.

As programs and initiatives develop, significant coordination at the state level will advance the cybersecurity posture more effectively. In that effort, this report concludes the following:

- A service and teaching model, as in a teaching security operations center (SOC), can benefit both the community and students. As part of a larger array of tools for underserved organizations, a teaching SOC can be leveraged with the resources in private industry.
- Tools to assist underserved organizations are needed. Specifically, security risk assessment and decision making tools would provide significant value to assess the unique vulnerabilities of organizations.
- A better understanding of community needs would be helpful for developing the range of services that may be provided to underserved organizations. A more detailed study of underserved organizations is needed.
- Workforce development initiatives should focus on creating affiliation and commitment for future workers to stay in the state. Oregon-based initiatives and programs that couple high-level internships with post-graduation work or fellow opportunities can add value.
- Expanding teaching and instructional capacity should be a priority across all educational and workforce development initiatives. Options for expanding capacity including working with industry professionals in teaching and/or mentoring roles.
- A future funding strategy should be highly collaborative and include educational institutions and private industry. A convener with the capacity to sponsor a collaborative strategic funding initiative is needed. This process should develop a shared vision, roles, and steps for achieving significant funding over the next three to five years.

Introduction and Background

National, state, local agencies and associations articulate significant concern over the gaps in cybersecurity capacity. At the Federal level, the National Security Agency, Federal Bureau of Investigation, and Department of Homeland Security have major initiatives to address cybersecurity threats. Executive orders, national initiatives, and reports at all levels in the public and private sectors have documented the need for organizational capacity, services, coordination, and skilled workers.[i]

Oregon's Senate Bill 90 (ORS 276A.326-9), signed into law and effective as of July 1, 2017, in part, focused on building capacity through a Cybersecurity Center of Excellence (CCoE). The CCoE Establishment Plan, prepared by Portland State University's Center for Public Service in 2018 highlighted the need for additional cybersecurity services and qualified professionals throughout the state.[ii]

This report builds on the strategies identified in the CCoE Establishment Plan and other previous studies. This document is focused on a related, three-part strategy to increase capacity by understanding:

1. Best practices to provide cybersecurity services to underserved organizations in the state of Oregon
2. Best practices to develop the experiential opportunities to train cybersecurity workers
3. Funding opportunities to advance the cybersecurity posture in Oregon

This three-part strategy benefits both the public and private sectors by building capacity across sectors. It accepts the findings of previous studies that there is a lack of cybersecurity services available to underserved organizations, such as small businesses, tribes, and school districts. It also accepts the conclusion of other reports that there are opportunities to build the workforce through practical experiential educational programs. Finally, this report assumes that the goal of a workforce development strategy is to attract and retain workers for the benefit of the state of Oregon.

Best Practices for Cybersecurity Service Provision

Managed Security Service Providers (MSSP) and Security Operation Centers (SOC)

The purpose of this section is to better understand the services being provided in the cybersecurity arena. Increasing the availability of these services through a public or private model requires a better understanding of current availability and conditions. It then follows with a discussion related to the development of a SOC in general and in the university environment.

Cybersecurity Ventures' Steve Morgan argued that the global shortage in cybersecurity professionals will reach 3.5 million unfilled positions by the year 2021. Managed security service providers (MSSP) have stepped up to fulfill the growing necessity of cybersecurity with a portfolio of services that fit many organization's needs. These providers look to ensure that all elements in the network are "security aware". They aim to provide a flexible approach that suits different sizes of enterprise customers.

Managed security services work as a house alarm where security operations centers (SOCs) are the response team that helps to resolve issues or problems. These services are beneficial to organizations that have limited IT resources and lack internal security expertise.[iii] Since the cost and effort to build an in-house SOC exceeds the budget of many organizations, many decide to leave their security monitoring options to an MSSP.

Managed Security Services

A more comprehensive list of services appears in Appendix A of this document, however, the most common managed security services available include the following: [iv]

- Remote 24/7 monitoring of security events and security-related data sources
- The administration and management of IT security technologies
- The delivery of security operation capabilities via shared services (generally services do not include on-site personnel or remote services delivered on a one-to-one basis)

The core service of most MSSPs lie with the 24/7 security event monitoring and response for threat detection. Many also include other services in their portfolio, including[v]

- Security Technology Administration
  - Management of firewalls
  - Unified threat management (UTM)
  - Intrusion detection and prevention system (IDPS)
  - Endpoint protection platform (EPP)
  - Endpoint detection and response (EDR)
  - Secure web gateway (SWG) and secure email gateway (SEG)
- Incident response services (remote and on-site)
- Vulnerability assessment and managed vulnerability management services (e.g., scanning, analysis and recommendations/remediation)
- Threat intelligence services (e.g., machine-readable threat intelligence feeds, customer-specific dark web and social media monitoring)
- Managed detection and response (MDR) services

Managed Security Services Pricing Models

MSSPs use several different pricing models. Generally, pricing tends to be based on the type and size of the security technology to be managed. Pricing schemes appear to vary based on the following:

- log data collection and charge fees based on number or types of sources
- events per time period
- data volume or velocity
- total number of sources sending data to the MSSP
- number of incidents that are detected, number of alerts notified, the number of users, or the number of assets.[vi]

The most popular managed IT services pricing models on the current market include:

- Per-device pricing: A flat fee for each device that is supported
- Per-user pricing: Per-user pricing includes the number of users that require managed services
- "All inclusive" pricing: Costs associated with having the majority of networked services managed. This includes a subscription model where a flat fee for monthly costs are covered

Other fees are generally one-time fees. These include:

- Onboarding costs: This is a cost associated with switching to a MSSP, including such things as setup of VPNs (virtual private networks), network circuits, or other infrastructure
- Remediation costs: These include fees for hardware or infrastructure after managed services have launched[vii]

MSSP Fees

As part of the development of this report, the research team collected information on various pricing schemes. Because many providers price their services on the basis of individual quotes, limited information is available. As perhaps, expected, costs for monitoring range significantly. On the low end, companies offer limited support for log management, security monitoring, by IP's or per user. For example, AT&T Cybersecurity offers monitoring support to existing IT teams or SOCs with software tools. On the upper end, some providers offer robust 24/7 monitoring and management services. These pricing options are available upon request from the authors.

Analyzing MSSP fees and price points offers only limited usefulness, as service needs vary significantly among organizations. As a result, there is more work to be done to assess the general capacity of underserved organizations, their risk profile, and budget tolerance for security services.

MSSP Providers

One of the challenges for underserved organizations is having a limited understanding of which providers can assist in cybersecurity. The language and knowledge gap of small business creates delays in implementation as well as confusion.[viii] [ix] In an effort to bridge this gap, Mount Hood Community College has developed a list of trusted providers and will work with small businesses to plan for services. For the purpose of this report, Appendix B provides an initial list of MSSP and SOC providers. Future research should be dedicated to developing practical tools that allow organizations to model and assess their unique security risk in order to make decisions about the right mix of services.

Limitations and Gaps of Managed Security Service Providers

According to the Forrester Wave Reports for Security and Risk Professionals, there is a recognition that data analytics for customers should be provided. The analytical and educational component is an important gap that a public organization could provide. For example, one of the things that SOCs have the capacity to provide involves analyzing information to find patterns from attacks, usage, among other indicators.[x]

For example, the Oregon Research and Teaching Security Operations Center (ORTSOC) at Oregon State University can fill gaps in education and access to providers. It may also provide some MSSP services through a service and teaching model. ORTSOC has capabilities that can help research and detect threats, get involved with metrics and deliver in threat intelligence / incident remediation (TIIR) and help develop better risk and compliance management (RCM). This report now turns to findings on developing a SOC in general.

Developing a Security Operation Center (SOC)

Before engaging in a discussion on best practices, it should be clarified that SOCs have particular tasks and activities for security and risk management. The SOC is designed to dedicate the organization to prevent, detect, assess, and respond to cybersecurity threats and incidents, as well as fulfill and evaluate regulatory compliance.

Building a SOC requires an organization that will be fully operational on a regular basis with a dedicated team and facility. Some SOC operations require 24/7 staffing. Some also consider a hybrid model, where the SOC may choose to use MSSP services available in the private market to offset costs. Several options for building a SOC, including a hybrid approach are outline in the draft HEISC Working Group Paper: Security Operations (SOC) Case Study.[xi]

Best practices of SOCs in Institutions of Higher Education

The CCoE Establishment Plan notes that workforce development initiatives, training for non-technical employees on cybersecurity best practices, and multi-sector engagement are vital for an Oregon cybersecurity strategy. As shown in Figure 1: Cybersecurity Health Model below, the framework articulated in the Cybersecurity Needs Assessment centered on achieving effectiveness in three areas: cyber-hygiene, public security monitoring, and response and recovery.[xii] This framework can be compared with the best practices on SOCs in other higher education institutions.

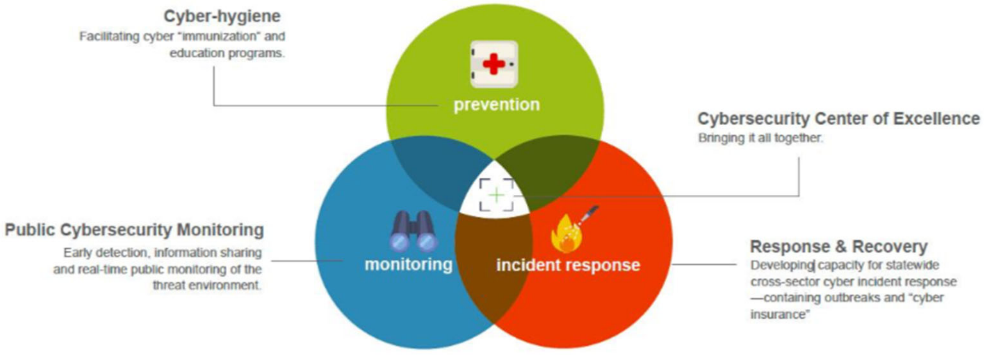

Cyber-hygiene
Facilitating cyber "immunization" and education programs.
prevention
Cybersecurity Center of Excellence
Bringing it all together.
Public Cybersecurity Monitoring
Early detection, information sharing and real-time public monitoring of the threat environment.
monitoring
incident response
Response & Recovery
Developing capacity for statewide cross-sector cyber incident response —containing outbreaks and "cyber insurance"

Figure 1: Cybersecurity Health Model

The following analysis assesses best practices in the following areas:

- Cybersecurity Operations
- Educational Opportunities
- Hands on Learning
- Employment and Research Collaborations
- Public Outreach

University of Texas at Austin

The University of Texas at Austin (UT Austin) operates a 24/7 monitoring center through the Department of Information Resources (DIR), offering Cybersecurity Operations for approximately 150 state agencies, higher education institutions and other public sector customers. DIR also looks for public outreach establishing a sustainable Cybersecurity Awareness Program. The SOC has a council that advocates and advises for public private partnerships with a goal of workforce development.

UT Austin also reaches out to the community to offer educational opportunities and training. University of Texas for example runs the program "we teach CS", which provides computer science training and provides with certificates of their learning to K12 teachers.

The Cybersecurity Operations Center (CSOC) conducts cybersecurity-related research and for the improvement of cybersecurity education. The Information security office has developed tools and processes to manage the most common cybersecurity operations. Vulnerability self-assessment, device inventory and log monitoring are among the tools that are available.[xiii]

Texas A&M

Texas A&M runs a cybersecurity program and aims to focus in two areas: Research collaboration and educational opportunities. Their research collaborations apply to areas such as critical infrastructure protection (energy, transportation, communication, interconnected and autonomous systems). The university works on the research and development of a cybersecurity workforce, privacy, and cyber ethics. More technical research involves specific topics such as malware, vulnerabilities on IoT, cryptography, and resilient systems.

Texas A&M offers cybersecurity certificates, bachelor's degree minors, and master's degrees. They also provide opportunities for hands on learning.

Since the state of Texas has an active monitoring program with a complete set of cybersecurity operations, Texas A&M's cybersecurity center focuses on workforce development and research.

University of Texas at San Antonio

The University of Texas at San Antonio (UTSA) is one of 10 centers nationally designated as a Center of Excellence in all three categories: Cyber Operations, Defense, and Research. As part of the University of Texas system, UTSA is part of a 5-Year Cooperative Research and Development Agreement funded by NSA. All institutions within the UT system can easily collaborate through joint work statements facilitated by the NSA agreement. Further NSA has a "specialized" agreement with UTSA for military and NSA civilian employees to complete their degrees. UTSA also engages in cooperative education program and summer internships, which allow NSA employees to attend school and work full time at NSA in rotations.[xiv] The UT system and UTSA is an excellent example of innovative partnerships that have the potential to advance the research, operations, and education in cybersecurity.

Maryland University College

In the state of Maryland, the department of information technology (DoIT), runs a 24/7 SOC which includes all the expected operations of a full-fledged operations center. This SOC takes advantage of its close proximity to the defense infrastructure, the NSA, the Defense Information System Agency, and U.S. Cyber Command.[xv]

Maryland Cybersecurity Center (MC2) in the Maryland University College performs interdisciplinary research, including economics, social sciences, computer sciences, and electrical engineering. Their focus is cryptography, software security behavioral aspects of security as well as cybersecurity economics. DoIT operates a 24/7 SOC for enterprise systems and other state government clients. This SOC is responsible for incident response and many cybersecurity operations.

MC2 offer bachelor's and master's degrees, and PhDs in computer sciences and electrical engineering. Public Outreach and workforce development are part of MC2, through corporate programs and collaborations, partners have "exclusive access" to recruit at undergraduate and graduate levels.

University of South Florida

The state of Florida created the Florida Center for Cybersecurity (FC2), which is a resource managed by the University of South Florida (USF) and shared with the other 11 universities. Their plan is to facilitate multi sector capacity building, while providing outreach, education, research and workforce development. Cyber Florida does not offer a SOC as a service has an active monitoring program, with a laboratory and simulation. Recently they acquired a security information and event management (SIEM) platform to improve their cyber incident reporting and information sharing processes.[xvi]

FC2 at USF offers opportunities for degrees as well as continuous professional development. It emphasizes hands-on learning to acquire experience and workforce development.

University of West Florida

The University of West Florida (UWF) is a member of the FC2 as well as the National CyberWatch Center. UWF operates through the Center for Cybersecurity, which acts as a regional hub. Education through hands on training is emphasized. UWF offers interdisciplinary cybersecurity programs and certificates. The undergraduate and graduate programs as well as the certificates are based on a multidisciplinary educational curriculum. This includes Computer Science, Information Technology, Information Security Management, Computer Engineering, Security and Diplomacy, Public Policy, among other related areas. The UWF offers a M.S. degree in Cybersecurity in an online format.

Similar to USF, UWF uses the same laboratory to work on simulations, with hands-on education and training. Besides partnering with universities and federal and state agencies, they aim for a continuous outreach to encourage and promote cybersecurity with the community.

Benefits of a University Based SOC

One of the purposes of a university-based SOC is to fill the service gap in the state while providing meaningful experiences for students. A SOC has the potential to provide services to public agencies as well as those that are currently underserved.

The primary question then, is how to appropriately target those that are underserved or are seen as unprofitable for private service providers such that it adds to the collaborative array of services. The ultimate goal is to identify gaps in service and find ways to fill those gaps.

Based on information available we know the following:

- 56% of for profit and nonprofit entities in Oregon are small, having 1 to 499 employees
- small businesses employ over half of Oregon state's workforce with approximately 85.000 small businesses[xvii]
- there are approximately 25.000 nonprofits in the state[xviii]
- the state has 221 school districts that cater more than half a million students[xix]

Many of these small and nonprofit organizations require assistance across the education, managed security, and information technology areas. There is also a lack of understanding of what kind of services that are needed and why they should fund these activities.

There appear to be a range of options available for moving forward, such as:

- providing solutions to underserved organizations by packaging solutions that do not rely exclusively on active monitoring and may include such things as, training for IT professionals and non-technical staff, internships, and public outreach to practice online safety
- build a SOC in a collaborative approach, such as partnering with private industry to cover gaps in service provision or comprehensive services
- providing guidance for underserved organizations by offering other tools, such as risk assessment models and tutorials to demystify complex terminology

SOC-Related Implications and Opportunities

At the heart of this discussion is how Oregon institutions can deliver services to underserved organizations while offering experiential educational opportunities for students. This section focused on the common services and operation of SOCs and best practices from university-based programs. While not all university programs offer SOC services, there are several best practices that can be useful to the state.

- A service and teaching model, as in a teaching SOC, can benefit both the community and students. The University of Texas at Austin provides a good example of a well-developed SOC within an educational institution.
- Institutional collaboration can offer significant advantages for attracting funding opportunities. The University of Texas system, for example, has attracted support from the NSA for a state-wide collaboration that leverages research with student education and cooperative work programs.
- The development of a SOC using a service and teaching model can be advanced through collaboration with private industry.
- Tools to assist underserved organizations are needed. Specifically, security risk assessment and decision making tools are needed. Many organizations need assistance in assessing their unique vulnerabilities. This may come in the form of simple documents or one-on-one consultations.
- A better understanding of community needs would be helpful for developing the range of services that may be provided to underserved organizations. For example, it is unclear whether underserved organizations need more education, planning assistance, or direct services. A detailed study of underserved organizations is needed.

Workforce Development: Best Practices for Internships and Practical Skill Development

Workforce Development and Education

The CCoE Establishment Plan described a variety of issues and opportunities related to workforce development. One of the strategies identified the CCoE Plan was to better understand and coordinate the educational systems through which the workforce is developed. This requires a better understanding of the constellation of training and educational efforts - including certifications and degrees at all levels.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) aims to provide a taxonomy describing cybersecurity work (see overview in Appendix C). The Framework consists of categories, specialty areas, work roles, and capability indicators. The NICE Framework is intended for use by employers, workers, technology providers, and educational institutions (including advisors, certification, and educational providers).[xx] The NICE Framework attempts to make sense of the complex range of workforce needs in cybersecurity. However, some argue that there are additional knowledge, skills, and abilities beyond the NICE Framework that are required for a successful cyber workforce.[xxi] Specifically, social and teamwork proficiencies are needed for a strong security posture. It is in advancing both the technical and social dimensions that experiential education can and should play a role.

Internships and Experiential Learning Best Practices

Workforce development in many practical and applied fields typically requires some combination of academic and hands-on (experiential) learning. This is because the context and nuances of applied work are not always captured in an academic setting. As a result, many degree programs require some kind of internship or experiential learning component. This approach is consistent across applied fields, such as in medicine, education, business, policy and cybersecurity.

Experiential learning is generally considered advantageous for several reasons. From a developmental perspective, students can directly apply their knowledge, access quick feedback, reflect on theory, and gain exposure to the work environment (such as working in teams or an organization’s culture). A recent New York Times article argued that classrooms are not effective for teaching for cybersecurity jobs because they cannot mimic the ‘disruptive, rebellious, and troublemaking instincts of the best security professionals’.[xxii] Embedding students in applied work also has the advantage of sponsoring agencies being able to leverage new and innovative knowledge that the students bring from the classroom.

There are a variety of best practices for internships and experiential learning in general, which are addressing in the following discussion.

Experiential Learning Goals

There are a variety of goals that can be achieved through experiential / internships, including:

- **Develop and retain the workforce for service in the state of Oregon**. One of the more significant challenges in the cybersecurity industry nationally is a shortage of skilled workers. As a result, in-demand professionals may choose to go elsewhere for work. This means that building capacity in the workforce should involve strategies to build affiliation and commitment to staying and serving in Oregon.

- **Increase the skills of existing employees** (both mid-career and lesser-skilled workers). The National Governor's Association argued that, "some employers simply need skilled workers who understand risk assessment and can utilize security applications – skills that can be taught to IT professionals who want to advance their career, or to lesser-skilled workers who want to enter a new field."[xxiii] Experiential learning opportunities can leverage employees existing jobs with educational support to advance the skills of committed employees.
- **Develop the workforce pipeline**. Developing a workforce pipeline of students includes those who are entering or already engaged in academic programs. This pipeline also includes those who are in k-12 institutions. K-12 institutions are primarily outside the scope of this report.
- **Increase diversity**. Building capacity of the workforce through experiential education may also include opportunities to increase gender, racial, and ethnic diversity in the field.
- **Develop instructional capacity**. This report also considers that one of the benefits of experiential learning is related to increasing instructional capacity beyond the academic setting. Internship supervisors, industry professionals, and senior practitioners can play important roles and extend the instructional capacity of the classroom.

Experiential Learning Approaches

Based on this best practice research, there are a variety of approaches to increase the practical skills needed in the cybersecurity field. These approaches can be combined to fulfill the dual needs of students and industry. The following discussion describes these models and assesses them for their likely effectiveness in an agency; the type of projects; the stage of education or training; and whether the experience is appropriate for individuals, teams, or organizations. This is summarized below in Table 1: Internship Models, on page 16 of this document.

Different models suggest that there are phases for knowledge, skill, and experience development. For example, the CERT Division of the Carnegie Mellon Software Engineering Institute uses a Four-Phase model to build on an individual's ability with increasing focus on real-world on-the-job experiences.[xxiv] These different experiential approaches can be arrayed on a continuum from more emphasis on close faculty guidance to increasing levels of responsibility. Figure 2: Increasing Level of Student Independence, below, demonstrates this array.

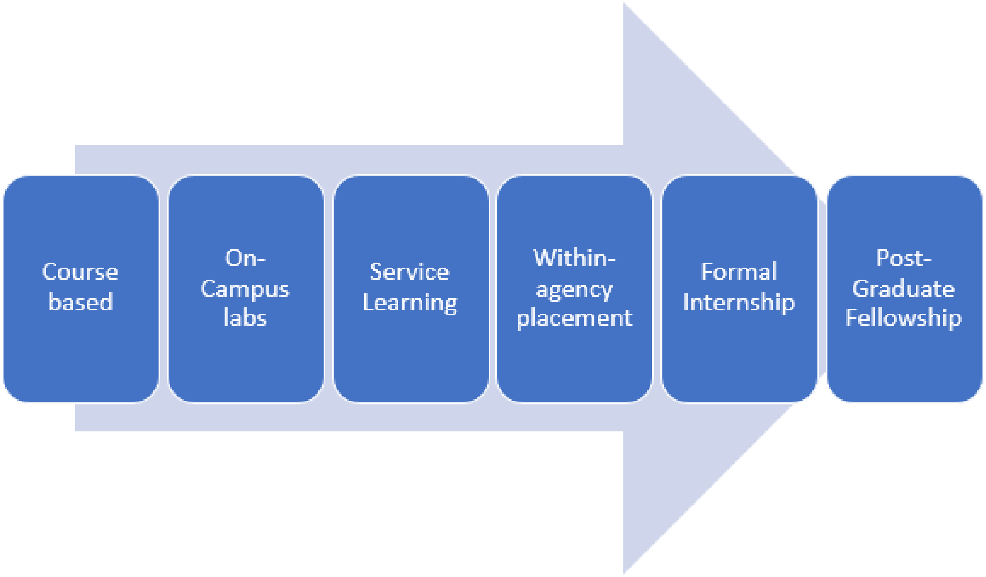


Figure 2: Increasing Level of Student Independence

Course-based learning. Many applied learning programs embed experiential learning activities into courses. This approach allows instructors to apply theory to real-world problems in a structured and intentional way. For example, Oregon Tech integrates hands on learning into the classroom through, 'real-world experiences.'[xxv] Other course-based learning approaches include projects in which the class solves problems brought to them by external organizations or the community. Depending on these types of experiences, an instructor might assign this to one student individually or to teams.

On-campus centers or learning 'labs' (SOC). On-campus learning centers describe such entities as the SOC, discussed above. Typically, centers or institutes attract external funding for projects or services and utilize students as a part of their staffing mix. These university-based centers or institutes have advantages for accommodating the educational needs of students moving through their degrees while providing a service to organizations. Centers have the advantage of accommodating a wide range of scopes and project sizes to students at all stages of their academic program, while utilizing individual, team, and organization-wide talent. Oregon State University's ORTSOC is an example of this approach in the cybersecurity arena.

Service learning. Service learning projects encompass a wide variety of activities that may or may not be directly supervised by an instructor. Service learning projects often take place outside credit-bearing classes and are often unpaid. Some institutions may require service learning hours that must be taken prior to graduation. The advantage of service projects is that they offer significant variety and are adaptable for individuals, teams, or organizations. Service learning projects vary in their direct connection to academic training, however, because reflection on the applicability of theory may be absent. Due to the independence associated with a service project, they are more appropriate for students in the latter stage of their training. For example, Mount Hood Community College's Oregon Center for Cybersecurity provides small businesses with a student partner that assists with identifying security needs and connecting with security providers.[xxvi]

Within-agency training and mentoring. Another type experiential learning targets students who are already working in an organization but for whom may desire to advance their career or gain new technical skills. This type of experiential learning is often known as cooperative education. It focuses on the organization as the basis for work. The role of academic program would be to support students through academic coursework. Though institutions of higher education may not be directly organizing this experiential learning, they may be support students by offering flexible classes in the evening, weekend, or online in order to accommodate student schedules. The advantage of this approach is that students' learning is embedded in their organization and, presumably, have some affinity towards its success.

Formal external internship placements. Formal internships are hosted by a wide variety of public and private organizations. These placements often have a mentor or highly skilled employee who can supervise students. The placements have a number of advantages in that they offer the opportunity for students to become embedded in organizations, agencies to test out potential talent, and the expansion of staffing. However, external placements often require organizational capacity to supervise students, which may not be possible in smaller or otherwise underserved organizations. Due to the somewhat limited timeframe of an internship, if a project is large or ongoing, the internship scope or tasks should be somehow limited.

Oregon State University, Oregon Tech, Portland State University, and University of Portland have a relationship with MECOP Inc., (formerly known as the Multiple Engineering Cooperative Program) where industries provide input into the university curriculum and host interns in a six-month timeframe.[xxvii]

There are several best practices that can also be considered when placing students, including summer internship and rotational assignments.

> *Summer internships.* Summer internships offer student the opportunity to productively engage in applied work while on a break from their academic studies. There are a number of agencies that offer summer internships in the public and private sector. Many times, summer internships offer the opportunity for a post-graduation placement. The advantage to agencies is clear in that they can 'test out' talent, acculturate students to their organization, and provide training suited to the context. There are several federal programs that offer formal internships, including the Department of Homeland Security, Federal Bureau of Investigation, and the Central Intelligence Agency.[xxviii]
>
> *Rotational approach*. Rotational internships require students to move through several different placements. This is similar to a medical doctor training program where the variety of organizational contexts increase the adaptability and knowledge of the student. For example, Portland State's Computer Science program rotates students through formal internship program through the Multiple Engineering Cooperative Program (MECOP) and the PSU/PDX Cooperative Education Program (PCEP). PSU requires two six-month, full-time internships at two different companies in student's junior and senior years. The PCEP is a half-time, year-round internship that rotates among PCEP member companies every six months, beginning in student's junior year.

Post-graduate fellow programs. The last category of internship best practices is post-graduate fellowships. These positions are generally categorized as early career positions. The advantage to these opportunities is that agencies can attract highly skilled individuals immediately after graduation. Some offer additional training, mentoring, professional development, and departmental rotation. Currently, the Department of Homeland Security and Federal Bureau of Investigation offer such opportunities. Oregon agencies may consider such a program as a way to attract and keep talent in the state.[xxix] More than likely, a fellowship program is more viable for larger public or private entities, due to the intensive resources that may need to be applied. On the other hand, a creative multi-university collaboration may provide an opportunity for graduate to rotate among several organizations.

Table 1, below, summarizes these various internship models.

Table 1: Internship Models

	Agency Setting	Project Scope	Stage of Student's Education or Training	Appropriate
Course-based	Underserved Public Private	Limited scope	Early Mid Late	Individual Team
Campus-based Centers	Underserved Public Private	Limited scope On-going services Large or multi-year projects	Early Mid Late	Individual Team Organization
Service Learning	Underserved Public Private	Limited scope Large multi-year projects	Late	Individual Team Organization
Within-agency Training and Mentoring	Public Private	Limited scope On-going services Large or multi-year projects	Early Mid Late	Individual
Traditional / External Placements	Public Private	Limited scope	Mid Late	Individual
Fellowships	Underserved* Public Private	Limited scope On-going services Large or multi-year projects	Late	Individual

Due to the limited scope of this report, a comprehensive inventory of higher educational institutions offering experiential education was not possible. However, the initial findings indicate that course-based and formal internships are most commonly used. Several institutions offer some kind of service learning opportunity where students engage in projects or clubs that provide value to the community. Finally, based on the preliminary findings, it appears that Klamath Community College and Oregon State University are including students in collaborative projects with community entities. A preliminary list of experiential opportunities appears in Appendix D.

Challenges

Providing experiential education opportunities is extremely rewarding but presents several challenges in the cybersecurity arena. These include challenges in placement, labor laws, host mentor capacity, and onboarding and security.

Placement. Placing students in internships can be challenging for any field. This requires at least one individual at the academic institution to have good outward-facing community relationships with agencies, businesses, or communities. Some institutions hire an internship coordinator for this purpose and others place the responsibility on faculty. Other models post openings for students to apply on their own. For example, PSU Hosts an archive of available jobs and internships.[xxx]

Host Mentor Time and Availability. External internships also require that the host agencies have mentors available to supervise interns. This is not always available in smaller or underserved agencies, who may have limited or no technology or cybersecurity staff. Without intervention, these agencies will have limited opportunity to host an intern unless there is external guidance or supervision available. A related challenge is related to diversity in mentors. Some have noted that having a mentor that can relate to their experience is essential for continued career development.[xxxi] However, it is unclear that these mentors are consistently available.

Onboarding and Security. Other challenges associated with internships involve hiring and onboarding. Many organizations have onboarding requirements for workers, even if they are unpaid. This is most important for those organizations that will give the individual access to sensitive information and networks. As a result, shorter term internship placements may be difficult and time consuming to manage, depending on the complexity of the project.

Resources for Experiential Learning

There are a variety of resources available to fund student placements in applied settings. These range from Federal grants to support from private industry. Several models are described below.

Federal grant support. There are several grants that are available to institutions of higher education that are specifically designed for student scholarships. The CyberCorps Scholarship for Service grant provides considerable support for students. A critical component of these grants is that the student serves in an internship capacity during their summer breaks and that they work after graduation for a federal, state, local, or tribal Government organization for a period equal to the length of the scholarship. The host institution must also have a "clearly documented evidence of a strong existing academic program in cybersecurity" in most instances that comes through designation as a Center of Academic Excellence in Cyber Defense (Education and Research) CAE-R or Operations (CAE-CO).[xxxii] [xxxiii] An additional designation is awarded to two-year colleges (CAE-2Y). According to the National IA Education and Training Programs, these designations in Oregon are:

- Mt. Hood Community College CAE-2Y 2014-2019
- Portland Community College CAE – 2Y 2018-2023
- University of Oregon CAE-R 2014-2019

There are no educational institutions in Oregon that are designated as Cyber Operations Centers of Excellence.

University based fee for service. Another source of support for student's experiential work is through centers and institutes that may receive funding for services or fees. Depending on the institutional structure, many Oregon universities have self-support activities that receive fees for performing services. The funds that are received for services through intergovernmental agreements or grants can be expended on personnel, including faculty and students, in the form of stipends or wages.

Agency support. Agencies may also choose to support particular students through their applied experiences. There is significant potential for agencies to sponsor students modeled after the Federal CyberCorps grant. A potential grant my require the student to serve in Oregon post-graduation. There may be significant value for an agency to invest in a well-prepared student. This has the potential to build affiliation with the agency as well as deliver a highly skilled employee with diverse skills. This approach could be open to public, private, and nonprofit agencies throughout the state.

Additional Considerations in Workforce Development

While this report focuses on the role that experiential education and internships can play in workforce development, there are significant concerns related to the lack of instructional capacity and an inadequate supply of students.

Expanding teaching capacity may include,

- Expanding the adjunct teaching pool by partnering with industry professionals who may possess the skills but lack formal qualifications to teach.[xxxiv] PSU is engaging in creative ways to use industry professionals in the classroom as a means to expand the capacity of existing faculty.
- Allowing private industry professional to train credential instructors in K-12 who already have an interest but lack specific cybersecurity skills.[xxxv] This may be a national, credentialing issue to solve, however, partnerships with industry to train K-12 instructors may have an opportunity at the local level to gain the needed technical skills along the way to credentialing.

Developing a more skilled workforce involves a range of ideas, including the following,

- Expanding the pipeline of students at an earlier age by interesting students in elementary through middle school and enhancing coding competitions and logic games.[xxxvi] [xxxvii] Some of this is already occurring throughout the state, such as the NW Cyber Camp. There may be federal grant opportunities to continue and extend this work.
- Working with credentialing agencies and private companies to make it easier for non-traditional institutions to credential participants (e.g., coding boot camps and competitions).[xxxviii]
- Developing a Civilian Cyber Corps that would perform similarly to civil reserve corps.[xxxix] This approach may be something that could be an Oregon-based pilot program, given appropriate funding, training, and coordination.

Implications and Opportunities for Educational Initiatives

The focus of this aspect of the report has been on providing students a range of opportunities to acquire direct hands-on experience while meeting the needs of organizations throughout the state. This report highlights the various categories of experiential education that can serve as a foundation for a prepared workforce that may be of use to academic programs and agencies. There are several opportunities that, if developed, can form the basis for an effective strategy. These are:

- Create affiliation and commitment for future workers to stay in the state through experiential educational placements. Make affiliation and commitment to the state an explicit goal of a formal placement.
- Build soft skills in teamwork and leadership along with technical skills. Most forms of experiential education can help develop a well-rounded professional.
- Consider an Oregon-based cyber corps and scholarship program for students that couples summer internships with post-graduation work or fellow opportunities.
- Create opportunities for private industry to sponsor students throughout their educational experience.

- Consider the use of on-campus labs or centers for appropriate cyber security projects as a way to provide paid opportunities for student training.
- Expand teaching capacity by opening pathways for industry professionals to serve in a teaching and/or mentoring capacity. Allow opportunities for experienced professionals to engage in adjunct teaching, mentoring, classroom/campus based projects, or other creative ways that extend instructional capacity. This is likely not the only answer to expanding the instructional pipeline, it may help to relieve the pressure on existing faculty.

Funding Sources and Strategy

In late 2018, the CcoE Establishment Plan conducted a funding search that identified a range of small to large funding opportunities from public and private sources. The funding sources have not changed significantly, however, some additional sources were identified. The funding document is available separately for future use. The following section is focused on the initial steps to develop a funding strategy that would better position entities in the state to attract larger grants.

Building off of the findings of this report, there are several strengths and opportunities that form the basis for a significant funding strategy.

Funding Strengths

- State entities, such as the Office of the State Chief Information Officer, are supportive of initiatives to advance the security posture in the state.
- Oregon educational institutions are highly collaborative and willing to work together.
- The Oregon Cybersecurity Advisory Council (OCAC) is supportive and has significant industry reach
- There are clearly identified workforce and service provision priorities in place, such as those documented in this report and in the CcoE Establishment Plan.

Funding Opportunities & Recommendations

Despite the significant strengths, there are additional opportunities that can better position individual and collaborative entities to attract large grant funds. The steps that may be taken to take advantage of the position of the state are as follows:

- Identify a convener to host a collaborative strategic funding initiative for educational entities in the state. Consider developing a shared vision, roles, and steps for achieving significant funding over the next three to five years.
- Identify the unique educational niche(s) filled by institutions and assess the ability to cover gaps. For example, there is variation among institutions that focus on research, technology, operations, and/or policy. Having a greater understanding of this variation may provide clarity for how to position the state overall relative to large federal granting agencies.
- Consider a formal educational institutional collaborative, using the University of Texas as a model.
- Work with private industry for large research initiatives to attract grant funds. For example, NSA funding is available for Industry-University Cooperative Research Centers that funds annual planning grants and long term initiatives.
- Coordinate a strategy among institutions to target federal grants for workforce development, research, and operations.

Considerations for Moving Forward

The goal of this report was to better understand how to both meet the needs of organizations while advancing workforce development. If successfully achieved, each could significantly increase the cybersecurity posture in state.

As programs and initiatives develop, intentional coordination will advance the cybersecurity posture of the state more effectively. In that effort, the following should be considered:

- A service and teaching model, as in a teaching SOC, can benefit both the community and students. As part of a larger array of tools for underserved organizations, a teaching SOC can be leveraged with the resources in private industry.
- Tools to assist underserved organizations are needed. Specifically, security risk assessment and decision making tools would provide significant value to assess the unique vulnerabilities of organizations.
- A better understanding of community needs would be helpful for developing the range of services that may be provided to underserved organizations. A detailed study of underserved organizations is needed.
- Workforce development initiatives should focus on creating affiliation and commitment for future workers to stay in the state. Oregon-based initiatives and programs that couple high-level internships with post-graduation fellowships can add value.
- Expanding teaching and instructional capacity should be a priority across all educational and workforce development initiatives. Options for expanding capacity including working with industry professionals in teaching and/or mentoring roles.
- A future funding strategy should be highly collaborative and include educational institutions and private industry. A convener is needed to sponsor a collaborative strategic funding initiative where a shared vision, roles, and steps for achieving significant funding over the next three to five years can be achieved.

Appendix A: Services of MSSPs / SOCs

Common services and components to run a SOC include:[1]

- Security Monitoring
  - Intrusion Detection/Prevention Systems
  - Anti-Virus
  - Data Loss Prevention
  - Vulnerabilities
  - Incident Tracking
- Vulnerability Management
  - Vulnerability Mitigation
- Incident Management
- Communications and Reporting
- Event and incident investigations
- Incident Handling
  - Incident Analysis
  - Incident Response
- Vulnerability Handling
  - Vulnerability Analysis
  - Vulnerability Response
- Forensics Analysis
  - Evidence Handling
  - Evidence Analysis
- Penetration Testing

- Security Technology Administration:
  - Management of firewalls,
  - Unified threat management (UTM),
  - Intrusion detection and prevention system (IDPS),
  - Endpoint protection platform (EPP),
  - Endpoint detection and response (EDR),
  - Secure web gateway (SWG) and secure email gateway (SEG)
- Incident response services (both remote and on-site)
- Vulnerability assessment and managed vulnerability management services (e.g., scanning, analysis and recommendations/remediation)
- Threat intelligence services (e.g., machine-readable threat intelligence feeds, customer-specific dark web and social media monitoring)
- Managed detection and response (MDR) services

[1] Building-a-Cyber-Security-Operations-Center-—-Lessons-Learned.pdf

Appendix B: Notable MSSP Providers

Companies with National Reach

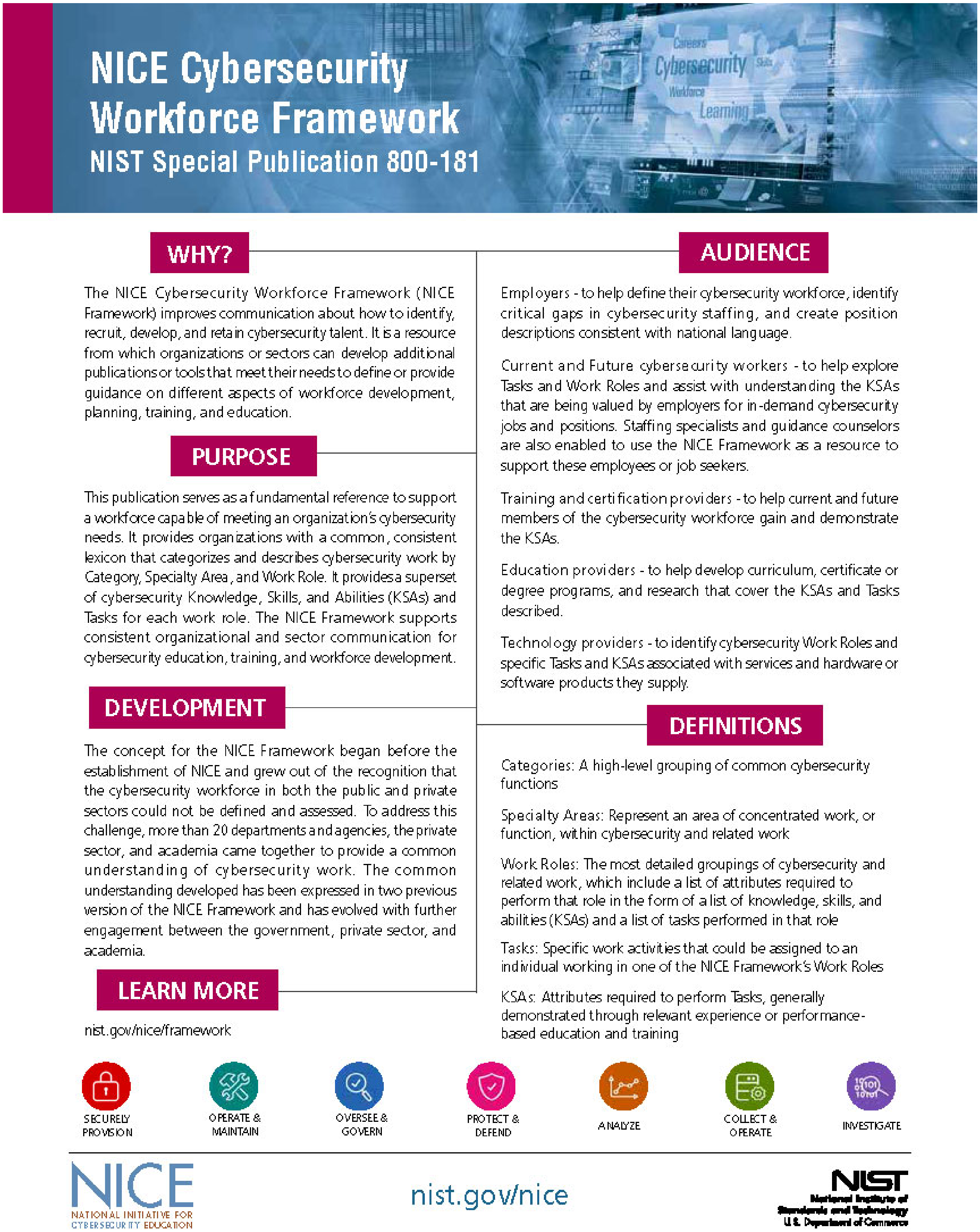
- SecureWorks provides a range of security event monitoring and response services. They also work on consulting for technology management, vulnerability assessment and management. This company works via retainer for incident response, which provides proactive as well as remote and on-site reactive response services.
- Trustwave offers conventional managed security services such as 24/7 security event monitoring and vulnerability management, as well as Managed Detection and Response (MDR). This company aims to work with midsize enterprises to large, global enterprises, that need to standardize its security
- AT&T Cybersecurity offers a range of security device management, and security monitoring and response services for large enterprises, midsize businesses and governments, it uses the approach of “follow the sun” to offer 24/7 security monitoring with their four SOCs.
- CenturyLink is a telecommunications and public and private cloud service provider with 8 SOCs that service small and large organizations. This provider has several service tiers available, from basic endpoint security management to advanced threat-oriented capabilities, and the pricing model for MSSs depends on the services contracted. CenturyLink also offers free log ingestion of 10 Gb per day, incident response services for managed firewall customers with no retainer.
- Alert Logic’s services are focused around 24/7 security event monitoring, threat detection and response, and vulnerability management of public and private cloud services (i.e., IaaS), as well as on-premises and hybrid environments. They offer three tiers of services — Essentials, Professional and Enterprise — that are aimed at a range of buyers, from midsize enterprises to large, global enterprises.

Oregon Based Companies

Some companies based in the State of Oregon offer solutions typically tailored for small enterprises and non-profits. These companies can likely scale to medium size organizations as well. They do not operate SOCs at the scale of the global MSSPs, although their personnel are able to work on security and disaster management.

- Arctic MSP
- Meta Technology Solutions
- Polar systems
- BendCloud
- Convergence Networks
- Proficio
- Expel
- Anitian
- TripWire

Appendix C: NICE Framework


Careers
Cybersecurity
Skills
Workforce
Learning

NICE Cybersecurity Workforce Framework

NIST Special Publication 800-181

WHY?

The NICE Cybersecurity Workforce Framework (NICE Framework) improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

PURPOSE

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work by Category, Specialty Area, and Work Role. It provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

DEVELOPMENT

The concept for the NICE Framework began before the establishment of NICE and grew out of the recognition that the cybersecurity workforce in both the public and private sectors could not be defined and assessed. To address this challenge, more than 20 departments and agencies, the private sector, and academia came together to provide a common understanding of cybersecurity work. The common understanding developed has been expressed in two previous version of the NICE Framework and has evolved with further engagement between the government, private sector, and academia.

LEARN MORE

nist.gov/nice/framework

AUDIENCE

Employers - to help define their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and create position descriptions consistent with national language.

Current and Future cybersecurity workers - to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. Staffing specialists and guidance counselors are also enabled to use the NICE Framework as a resource to support these employees or job seekers.

Training and certification providers - to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs.

Education providers - to help develop curriculum, certificate or degree programs, and research that cover the KSAs and Tasks described.

Technology providers - to identify cybersecurity Work Roles and specific Tasks and KSAs associated with services and hardware or software products they supply.

DEFINITIONS

Categories: A high-level grouping of common cybersecurity functions

Specialty Areas: Represent an area of concentrated work, or function, within cybersecurity and related work

Work Roles: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

Tasks: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

SECURELY PROVISION

OPERATE & MAINTAIN

OVERSEE & GOVERN

PROTECT & DEFEND

ANALYZE

COLLECT & OPERATE

INVESTIGATE

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

nist.gov/nice

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Appendix D: Preliminary Inventory of Experiential Education Opportunities

	Course-based	Campus-based Lab / Center	Service Learning	Formal Internships
Eastern Oregon University	X			X
Klamath Community College	X	X	X	X
Lane Community College	X		X	X
Mt. Hood Community College	X		X	X
Oregon State University	X	X		X
Oregon Tech	X			X
Portland Community College (Sylvania)	X		X	X
Portland State University	X			X

Appendix E: Acknowledgements

This report was developed in collaboration with public and private industry professionals and students. We would like to thank the following for their generous contribution of time providing information, reviewing documents, or general support.

Rakesh Bobba, Oregon State University

William Brandsness, Klamath Community College

Richard Croft, Eastern Oregon University

Annalise Famigliette, OSCIO Office

Wu-Chang Feng, Portland State University

Kerri Fry, IGNW

David Howard, Arctic MSP

Marcus Ingle, Portland State University

Doug Jones, Portland Community College

Charlie Kawasaki, Pacstar

Jens Mache, Lewis & Clark College

Francisco Marin, Portland State University

Gary Meenaghan, Lane Community College

Dave Nevin, Oregon State University

Ruth Swain, Mt. Hood Community College / Small Business Development Center

Zander Work, Oregon State University

Terrence Woods, OSCIO

Candace Worley, McAfee

Members of the OCAC Education / Security Operations Center Work Group

Appendix F: End Notes

[i] For example, President Trump's May 2, 2019 Executive Order on America's Cybersecurity Workforce calls for a focus on developing the Federal workforce capacity see: https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/. See also Executive Order 13800, May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure and President Obama's Executive Order, Improving Critical Infrastructure Cybersecurity.

[ii] Banyan, Margaret, Marcus Ingle, Kent Robinson, Jess Daley, Isaac Butman, and Emily Vilorio, 2018. Establishment Plan for the Oregon Cybersecurity Center of Excellence. Oregon State Chief Information Office.

[iii] See: https://cybersecurityventures.com/managed-security-service-providers-mssps/

[iv] Gartner, Inc. https://www.gartner.com/it-glossary/mssp-managed-security-service-provider

[v] Charest, Kevin. Building a Cyber Security Operations Center. Retrieved 6-21-19 from https://hitrustalliance.net/content/uploads/2014/03/Building-a-Cyber-Security-Operations-Center-%E2%80%93-Lessons-Learned.pdf

[vi] See: https://www.esecurityplanet.com/products/top-managed-security-service-providers.html

[vii] See: https://www.paranet.com/blog/bid/128269/Cost-and-pricing-models-for-Managed-IT-Services

[viii] Personal conversation with Ruth Swain, Mount Hood Community College. 6-19-19.

[ix] Forrester-wave-managed-security-services-report-cm160514.pdf

[x] Ibid.

[xi] Higher Education Information Security Council (HEISC). June 2019. *Security Operations Case Study*. https://library.educause.edu/-/media/files/library/2019/6/HEISCsoc.pdf

[xii] Craven, R., 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. Center for Public Service Portland State University.

[xiii] University of Texas at Austin Information Security Office: https://security.utexas.edu/

[xiv] See description of UT San Antonio and NSA partnership at: https://www.nsa.gov/resources/students-educators/featured-schools/utsa/

[xv] See: http://www.cyber.umd.edu/about

[xvi] State of Florida. Agency for State Technology. Chief Information Security Office. Statewide Strategic Information Technology Security Plan 2015-2018 (2017 Update).February 2017. Pg 4.

[xvii] See: https://www.sba.gov/sites/default/files/advocacy/OR.pdf

[xviii] See: https://www.guidestar.org/search

[xix] See: http://oregon.educationbug.org/public-schools/

[xx] See "Using the NICE Framework" at https://niccs.us-cert.gov/sites/default/files/documents/pdf/using%20the%20nice%20framework_pdf.pdf?trackDocs=using%20the%20nice%20framework_pdf.pdf

[xxi] Dawson, Jessica, & Thomson, Robert. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Frontiers in Psychology, 9(744).

[xxii] Wolff, Josephine. 2018. How Do You Get Students to Think Like Criminals? The skills needed for cybersecurity jobs aren't easy to learn in the classroom. *New York Times* Opinion. November 14, 2018.

[xxiii] Blute, Thomas. Meet the Threat: States Confront the Cyber Challenge. National Governor's Association, May 2019. Retrieved: https://ci.nga.org/files/live/sites/ci/files/1617/docs/1610WorkforcePipeline.pdf

[xxiv] Baker, Marie. 2016. Striving for Effective Cyber Workforce Development. Software Engineering Institute Carnegie Mellon University. May 2016.

[xxv] See Oregon Tech's approach at https://www.oit.edu/academics/degrees

[xxvi] Op. Cit., Ruth Swain.

[xxvii] See MECOP program at: https://www.mecopinc.org/

[xxviii] See the Cybersecurity Internship Program at DHS: https://www.dhs.gov/homeland-security-careers/cybersecurity-internship-program-0 ; FBI Honors Internship Program at: https://www.fbijobs.gov/students/undergrad ; and the CIA Student / Co-Op Program at https://www.cia.gov/careers/student-opportunities/undergraduate-internships.html

[xxix] See the DHS Secretary's Honors Program at https://www.dhs.gov/homeland-security-careers/secretarys-honors-program; and the FBI's Collegiate Hiring Initiative at https://www.fbijobs.gov/students/undergrad

[xxx] See archive at https://intranet.cecs.pdx.edu/careers/archives/cs/

[xxxi] Gonzalez, Matthew D. Gonzalez, Matthew D. 2015. Building a Cybersecurity Pipeline to Attract, Train, and Retain Women, *Business Journal for Entrepreneurs. P*ages 21-41, Volume 2015, Issue 3.

[xxxii] See CyberCorps Scholarship for Service at https://www.nsf.gov/pubs/2019/nsf19521/nsf19521.htm. Note that the CAE-CO designation is transitioning into two categories: Fundamental and Advanced.

[xxxiii] See NSA/CSS Centers of Academic Excellence in Cyber Operations at https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/ Note that the CAE-CO designation is transitioning into two categories: Fundamental and Advanced.

[xxxiv] Op. Cit. Blute

[xxxv] Ibid.

[xxxvi] Ibid.

[xxxvii] Nelson, Janel. 2019. Beefing Up the Cyber Workforce: Attracting technical talent in high demand requires innovative thinking. *Signal*. May 2019.

[xxxviii] Ibid.

[xxxix] George I. Seffers. 2019. Calling for a Civilian Cyber Corps: Experts tout the benefits of an army of civilian hackers. *Signal*. May 2019.