Proposal for a New Academic Program

Institution: Oregon Institute of Technology
College / School: College of Engineering, Technology and Management
Department / Program Name: Management Department
Degree and Program Title: B.S. Cybersecurity

1 Program Description

a. Proposed Classification of Instructional Programs (CIP) number: 11.1003

Title: Computer and Information Systems Security

Definition: A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, scripting, systems analysis, networking, cryptography, security system design, applicable law and regulations, risk assessment and policy analysis, contingency planning, user access issues, investigation techniques, and troubleshooting.

b. Brief overview (1-2 paragraphs) of the proposed program, including its disciplinary foundations and connections; program objectives; programmatic focus; degree, certificate, minor, and concentrations offered.

The federal government recognizes the rapid growth in the gap between cyber threats and skilled cybersecurity professionals who are proficient in identifying, reporting, and responding to information system exploitations. As such, Executive Order 13800, Growing and Sustaining the Cybersecurity Workforce, calls upon public universities to "grow a dynamic and diverse cybersecurity workforce," which is aimed to, "improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats" (US-CERT, 2017).

The order stresses the importance of developing a diverse workforce through hands-on training delivered via work-based learning, internships, and virtual assessment environments. As the Northwest's premier public polytechnic university, Oregon Tech will develop well-rounded cybersecurity professionals through its proposed Bachelor of Science in Cybersecurity degree program.

The proposed B.S. in Cybersecurity is designed to produce graduates that will be ready to enter the workforce as entry-level cybersecurity practitioners, analysts, and penetration testers. Through the program, students will gain foundational knowledge in information systems with focused courses on vulnerability scanning, threat detection, system health reporting, and system defense operations. The curriculum will follow the core knowledge units designed for National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) prepared by the National Security Administration and the Department of Homeland Security. Furthermore, the curriculum will include topics established by the National Institutes of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) framework.

The program objectives are to:

a. Provide students with the knowledge and skills necessary to competently scan, assess, report, and mitigate cybersecurity threats, vulnerabilities, and exploits on information systems and technology.
b. Address the five core Management Department student learning outcomes:
    i. Communicate the major concepts in the functional areas of accounting, marketing, finance, information technology and management.
    ii. Describe the legal, social, ethical, and economic environments of business in an internal/external (global) context.
    iii. Solve organization problems, individually and/or in teams, using quantitative, qualitative, and technology-enhanced approaches.
    iv. Demonstrate professional communication and behavior.
    v. Apply knowledge of business concepts and functions in an integrated manner.
c. Meet the core program learning outcomes
    i. Describe the tactics, techniques, and procedures used throughout the vulnerability assessment process.
    ii. Evaluate risk in information systems and apply mitigation techniques to reduce impact to business operations.
    iii. Perform information system vulnerability scanning and report findings.
    iv. Identify information system exploits and apply proper incident response.

c. Course of study – proposed curriculum, including course numbers, titles, and credit hours.

This section includes the proposed curriculum for both the Portland-Metro and Klamath Falls campuses. The Cybersecurity curriculum includes the Management Department's core curriculum in support of the Department's mission to educate students in practical management principles across multiple disciplines. The curriculum is designed to give students maximum flexibility within the department as they explore which Management Department degree option is best for them.

The Management Department is exempt from the 36 / 45 general education rule at Oregon Tech (See Appendix C, Item A).

Klamath Falls Course Schedule:

BS in Cyber Security			
	NEW CURRICULUM		
Prerequisite	**Freshman Year - Fall**		
Math 100	MATH 111	College Algebra	4
	SPE 111	Public Speaking	3
WRI 115	WRI 121	English Composition	3
		Lab Science Elective	4
		TOTAL:	14
	Freshman Year - Winter		
College Level Math	ECO 201	Principles of Microeconomics	3
	MIS 102	Spreadsheet Lab	1
	MIS 145	Introduction to PC Hardware/Software	4
WRI 121	WRI 122	Argumentative Writing	3
MATH 111	MATH 112	Trigonometry	4
		TOTAL:	15
	Freshman Year - Spring		
	BUS 215	Principles of Management	3
MIS 145	MIS 251	Networking I	4
	MIS 275	Introduction to Relational Database	3
Math 100	MIS 285	Python Programming	4
		TOTAL:	14

	Sophomore Year - Fall		
Math 100	ACC 201	Principles of Accounting I	4
Math 111	MIS 118	Introduction to Programming in C#	4
MIS 145	MIS 273	Systems Administration I	4
WRI 122 and SPE 111	WRI 227	Technical Report Writing	3
		TOTAL:	15
	Sophomore Year - Winter		
	BUS 226	Business Law	3
MATH 111	MATH 361	Statistical Methods I	4
MIS 118 and MIS 275	MIS 218	Database Programming	4
	CYB 201	Cyber Security Fundamentals	3
WRI 227	PHIL 331	Ethics in the Professions	3
	or		
WRI 122 and 3 cr. Hum Electives	PHIL 342	Business Ethics	3
		TOTAL:	17
	Sophomore Year - Spring		
ACC 201	ACC 203	Principles of Managerial Accounting	4
MIS 145	MIS 240	Intro to Linux OS	4
BUS 215 or BUS 317	MGT 335	Project Management	3
College Level Math	ECO 202	Principles of Macroeconomics	3
SPE 111	SPE 321	Small Group and Team Communication	3
		TOTAL:	17
	Junior Year - Fall		
ACC 203	ACC 325	Finance	4
MIS 251	MIS 351	Routing and Switching I	4
WRI 121	MIS 311	Introduction to Systems Analysis	3
		Humanities Elective	3
CYB 201 and MIS 285 and WRI 227	CYB 301	Hacker Tools and Techniques	4
		TOTAL:	18
	Junior Year - Winter		
MIS 275 and MIS 311	MIS 312	Systems Analysis I	4
MIS 118 and MIS 275	MIS 341	Relational Database Design I	4
WRI 227	WRI 350	Documentation Writing	3

	or		
WRI 227	WRI 327	Advanced Tech Writing	3
MATH 361 and MIS 113 or MIS 275	MIS 334	Business Analytics	3
CYB 301 and MIS 351	CYB 302	System Defenses and Incident Response	4
		TOTAL:	18
	Junior Year - Spring		
	BUS 223	Marketing I	3
MIS 218, MIS 312, MIS 341	MIS 322	Systems Analysis II	4
MIS 312 and MGT 335	MIS 495	Senior Project Selection	1
CYB 301 and SPE 321	CYB 303	Security Operations and Analysis	4
CYB 201 and MIS 351	CYB 351	Network Security	4
		TOTAL:	16
	Senior Year - Fall		
MIS 251 and MIS 273	MIS 365	Cloud Computing	4
MIS 495 and MIS 322	MIS 496	Senior Project Mgmt	3
BUS 215 or BUS 304 and MIS 206 or MIS 311	CYB 411	Managing Risk in Information Systems	3
BUS 215, BUS 304, BUS 317	MGT 321	Operations Management	3
		TOTAL:	13
	Senior Year - Winter		
SPE 111 and WRI 122	BUS 356	Business Presentations	4
MIS 496	MIS 497	Senior Project I	3
Junior Standing or Instructor's Consent	PSY 347	Organizational Behavior	3
BUS 215, BUS 304, BUS 317	BUS 349	Human Resource Mgmt	3
		TOTAL:	13
	Senior Year - Spring		
MIS 497	MIS 498	Senior Project II	3
ACC 203 and WRI 227	BUS 478	Strategic Management	3
WRI 122	ANTH 452	Globalization	3
		Humanities Elective	3
		TOTAL:	12

		Degree Total	182

Portland Metro Course Schedule:

BS in Cyber Security			
	NEW CURRICULUM		
Prerequisite	**Freshman Year - Fall**		
Math 100	MATH 111	College Algebra	4
WRI 115	WRI 121	English Composition	3
	MIS 145	Introduction to PC Hardware/Software	4
MATH 100	MIS 285	Python Programming	4
		TOTAL:	15
	Freshman Year - Winter		
		Humanities Elective	3
	MIS 102	Spreadsheet Lab	1
MIS 145	MIS 251	Networking I	4
WRI 121	WRI 122	Argumentative Writing	3
MATH 111	MATH 112	Trigonometry	4
		TOTAL:	15
	Freshman Year - Spring		
College Level Math	ECO 201	Principles of Microeconomics	3
	SPE 111	Public Speaking	3
MIS 145	MIS 273	Systems Administration I	4
MATH 111	MIS 118	Introduction to Programming in C#	4
		Humanities Elective	3
		TOTAL:	17
	Sophomore Year - Fall		
Math 100	ACC 201	Principles of Accounting I	4
	BUS 215	Principles of Management	3
	MIS 275	Introduction to Relational Database	3
WRI 122 and SPE 111	WRI 227	Technical Report Writing	3
		Lab Science Elective	4
		TOTAL:	17
	Sophomore Year - Winter		

	BUS 226	Business Law	3
ACC 201	ACC 203	Principles of Managerial Accounting	4
College Level Math	ECO 202	Principles of Macroeconomics	3
	CYB 201	Cyber Security Fundamentals	3
WRI 227	PHIL 331	Ethics in the Professions	3
	or		
WRI 122 and 3 cr. Hum Electives	PHIL 342	Business Ethics	3
		TOTAL:	16
	Sophomore Year - Spring		
MIS 118 and MIS 275	MIS 218	Database Programming	4
MIS 145	MIS 240	Intro to Linux OS	4
BUS 215 or BUS 317	MGT 335	Project Management	3
SPE 111	SPE 321	Small Group and Team Communication	3
	BUS 223	Marketing I	3
		TOTAL:	17
	Junior Year - Fall		
MATH 111	MATH 361	Statistical Methods I	4
MIS 251	MIS 351	Routing and Switching I	4
WRI 121	MIS 311	Introduction to Systems Analysis	3
CYB 201, MIS 285 and WRI 227	CYB 301	Hacker Tools and Techniques	4
		TOTAL:	15
	Junior Year - Winter		
MIS 275 and MIS 311	MIS 312	Systems Analysis I	4
MIS 118 and MIS 275	MIS 341	Relational Database Design I	4
CYB 201 and MIS 351	CYB 351	Network Security	4
MATH 361 and MIS 113 or MIS 275	MIS 334	Business Analytics	3
		TOTAL:	15
	Junior Year - Spring		
ACC 203	ACC 325	Finance	4
MIS 218, MIS 312, MIS 341	MIS 322	Systems Analysis II	4
MIS 312 and MGT 335	MIS 495	Senior Project Selection	1
CYB 301 and SPE 321	CYB 303	Security Operations and Analysis	4
		TOTAL:	13
	Senior Year - Fall		

MIS 495 and MIS 322	MIS 496	Senior Project Mgmt	3
BUS 215 or BUS 304 and MIS 206 or MIS 311	CYB 411	Managing Risk in Information Systems	3
BUS 215, BUS 304, BUS 317	MGT 321	Operations Management	3
MIS 251 and MIS 273	MIS 365	Cloud Computing	4
		TOTAL:	13
	Senior Year - Winter		
SPE 11 and WRI 122	BUS 356	Business Presentations	4
MIS 496	MIS 497	Senior Project I	3
Junior Standing or Instructor's Consent	PSY 347	Organizational Behavior	3
BUS 215, BUS 304, BUS 317	BUS 349	Human Resource Mgmt	3
CYB 301 and MIS 351	CYB 302	System Defenses and Incident Response	4
		TOTAL:	17
	Senior Year - Spring		
MIS 497	MIS 498	Senior Project II	3
ACC 203 and WRI 227	BUS 478	Strategic Management	3
WRI 122	ANTH 452	Globalization	3
	or		
	HIST 452	Globalization and Pac NW	3
WRI 227	WRI 350	Documentation Writing	3
	or		
	WRI 327	Advanced Technical Writing	3
		TOTAL:	12
		Degree Total	182

d. Manner in which the program will be delivered, including program location (if offered outside of the main campus), course scheduling, and the use of technology (for both on-campus and off-campus delivery).

The proposed B.S. Cybersecurity degree will be offered to our on-campus students at both the Klamath Falls and Portland-Metro campuses, as well as to our online students. Lab equipment is available for both on-campus and online students. On-campus students will have direct access to equipment shared between Portland-Metro and Klamath. Online students will have access to private cloud infrastructure hosted by Oregon Tech and public cloud education services through Amazon Web Services paid subscriptions.

e. Adequacy and quality of faculty delivering the program.

All courses in the program are developed and are currently being taught by existing faculty. The faculty possess the necessary background and knowledge of course content to deliver courses effectively. Faculty and course review are conducted each time a course is offered. Departmental faculty members continue to receive excellent evaluations, including student evaluations, tenure, promotion, and post-tenure reviews. Part-time and adjunct faculty members teach some of the required courses, however, all adjuncts are reviewed carefully by the Program Director and Department Chair each quarter.

f. Adequacy of faculty resources – full-time, part-time, adjunct.

Full-time faculty:

Richard Bailey, Professor
(1991) Management. B.S. (1984), M.A. (1985) Utah State University. Certified Public Accountant

Sandra Bailey, Professor
(2000) Management. B.S. (1985) Utah State University; M.Ed. (2005) Oregon State University

Sharon Beaudry, Associate Professor, Business Program Director
(2014) Management. B.S. (1985) College of New Rochelle; J.D. (2009) Northwestern California University; M.B.A. (2013) Northcentral University. Senior Professional in Human Resources (SPHR)

Dan Carrere, Assistant Professor
(2017) Information Technology. B.S. (1998) M.MIS (2000) Georgia College and State University

Tracey Coon, Assistant Professor
(2018) Information Technology. B.S. (2011) Kaplan University; MSIT (2016) Southern New Hampshire University

Jeffrey Dickson, Associate Professor, IT Program Director, HI Program Director
(2010) Information Technology. B.S. (2006) Oregon Institute of Technology; M.B.A. (2012) Southern Oregon University

Jared Emard, Assistant Professor
(2016) Management. B.S. (2009) Oregon Institute of Technology; M.B.A. (2016) Southern Oregon University

Grant Kirby, Associate Professor

(2003) Management. B.S. (1987) Oregon Institute of Technology; M.B.A. (1999) University of Oregon; M.S. (2013) Portland State University; Graduate Certificate M.S. (2013) Portland State University

Carmen Morgan, Associate Professor, Accounting Program Director
(1989) Management. A.A. (1984), B.S. (1986) Oregon Institute of Technology; M.B.A. (1991) Portland State University. Certified Public Accountant: Oregon; Certified Management Accountant; Certified in Financial Management, Personal Financial Specialist.

Hallie Neupert, Professor, Department Chair
(1999) Management. B.A. (1994) Wellesley College; M.S. (1996) University of Arizona

Mike Pierce, Associate Professor
(2014) Management. B.S.C.E. (1978) University of Wisconsin-Platteville; M.B.A. (1992) Alaska Pacific University; Ph.D. (2002) Gonzaga University. Registered Professional Engineer: Wisconsin

Patrick Schaeffer, Associate Professor, Operations Management Program Director
(2009) Management. B.S. (1986), M.S. (1994) San Jose State University

Maureen Sevigny, Professor, Distance Ed Program Director
(1995) Management. B.A. (1976) Barnard College; M.B.A. (1978) New York University; Ph.D. (1995) University of Maryland

Lindy Stewart, Assistant Professor
(2015) Information Technology. B.S. (2012) Oregon Institute of Technology; M.S. (2015) Boston University

Kristy Weidman, Assistant Professor, Marketing Program Director
(2012) Management. B.S. (2001) Oregon Institute of Technology; M.A. (2006) Thomas Edison State University

Part-time faculty and Adjuncts:

Don DaSaro, Assistant Professor
(2008) Management. A.S. (1964) Metropolitan College; M.S. (1967) University of Missouri Science and Technology; M.B.A. (1991) Marymount University

Bren Rafaelly, Professor of Practice
(2017) Information Technology. B.S. (1995) Southern Illinois University, Carbondale; M.B.A. (1998) University of Phoenix

Laura Yates, Professor of Practice
(2015) Management. B.A. (1973) Portland State University; M.B.A. (2002) University of Oregon; DMgt (2011) George Fox University

g. Other staff.

The Management Department is supported by an Office Specialist 2 in Klamath Falls, an Office Specialist 2 in Portland-Metro, and staff in the Distance Education Department. No additional staffing will be needed to implement or support the program.

h. Adequacy of facilities, library, and other resources.

The Enterprise Technology and Cybersecurity (ETC) Lab provides equipment needed for students to complete the required lab exercises in the cybersecurity degree program. The lab environment is designed to allow students from the Klamath Falls and Portland-Metro campuses to have direct access to equipment. Additionally, it provides an outward facing connection to allow online students to establish a remote connection to the lab environment, allowing them to complete lab exercises in the same manner as on-campus students.

No additional library resources will be required to support the cybersecurity program. Existing journals and databases used by the IT and computer systems engineering technology programs will be more than adequate. No additional facilities are required. The cybersecurity students will share facilities and lab equipment with our existing information technology program students.

i. Anticipated start date.

a. Fall 2019 - Klamath Falls and Portland-Metro
b. Fall 2021 - Online

2 Relationship to Mission and Goals

a. Manner in which the proposed program supports the institution's mission, signature areas of focus, and strategic priorities.

Strategically, Oregon Tech wishes to build from its current areas of strength into programs that can leverage that expertise and expand the impact of the institution. Market demand, by both the student and industry, is essential to proposing and developing any new program. A Bachelor of Science program in cybersecurity fits perfectly into this framework. The information technology program is consistently ranked among the top IT programs nationally. The B.S. Cybersecurity degree draws heavily from and builds a solid foundation upon the strengths of the IT and Management programs and expands them into the highly in-demand field of cybersecurity. There is currently a critical global shortage of trained cybersecurity professionals, and there are no other programs specifically focused on the applied practice of cybersecurity anywhere in the state.

The proposed B.S. Cybersecurity degree is consistent with Oregon Tech's mission of providing high-

quality education combined with applied, real-world experiences to prepare graduates to enter the workforce as trained practitioners of their chosen discipline. This degree program focuses on creating well-rounded cybersecurity professionals. The B.S. Cybersecurity degree combines the necessary theory and frameworks to provide students with strong foundational knowledge, along with opportunities to apply their knowledge to real-world problems. Graduates of this program will have the required knowledge, skills and abilities needed to become successful professionals, with both a solid technical background and the "soft skills" that are necessary to succeed in today's work environment.

b. Manner in which the proposed program contributes to institutional and statewide goals for student access and diversity, quality learning, research, knowledge creation and innovation, and economic and cultural support of Oregon and its communities.

Oregon Tech has a strong commitment to first generation college students and providing access to those who might otherwise forgo higher education. Small class sizes and individualized focus help those who face challenges, both within and outside the institution. The cybersecurity program is designed to maximize access statewide by offering a variety of ways to engage with the program (Portland-Metro, Klamath Falls, online).

Oregon Tech is an integral part of the state and communities that it serves and has the potential to respond to localized areas of need. Cybersecurity services are costly, and sometimes out of reach for many small and mid-sized businesses. Oregon Tech will play a role in meeting some of that demand, as a service contribution in connection with providing students with realistic work experience in the CDC. Cybersecurity needs exist in every community across the state, and there are increasing threats to small and mid-sized enterprises as they become vectors to larger targets, for example as participants in the supply chain for our larger regional manufacturers. Cybersecurity arose as a critical topic at a manufacturing conference this spring, as manufacturing companies grapple with the implications of potential intellectual property theft, disruption to their production lines and other potential threats.

Oregon supports an industry cluster in cybersecurity, in the Portland-Metro region and statewide. Offering programs such as the B.S. Cybersecurity will support the workforce needs of those companies, making Oregon a more attractive place to locate. Access to local workforce education to support cybersecurity reduces recruiting and retention costs for industry participants, many of whom cite that hiring local is better because of the greater likelihood that those employees will stay.

c. Manner in which the program meets regional or statewide needs and enhances the state's capacity to:

Oregon Tech offering a B.S. in Cybersecurity meets regional and statewide needs by developing and mentoring graduates to be able to fill the current approximate 2,775 vacant cybersecurity jobs.

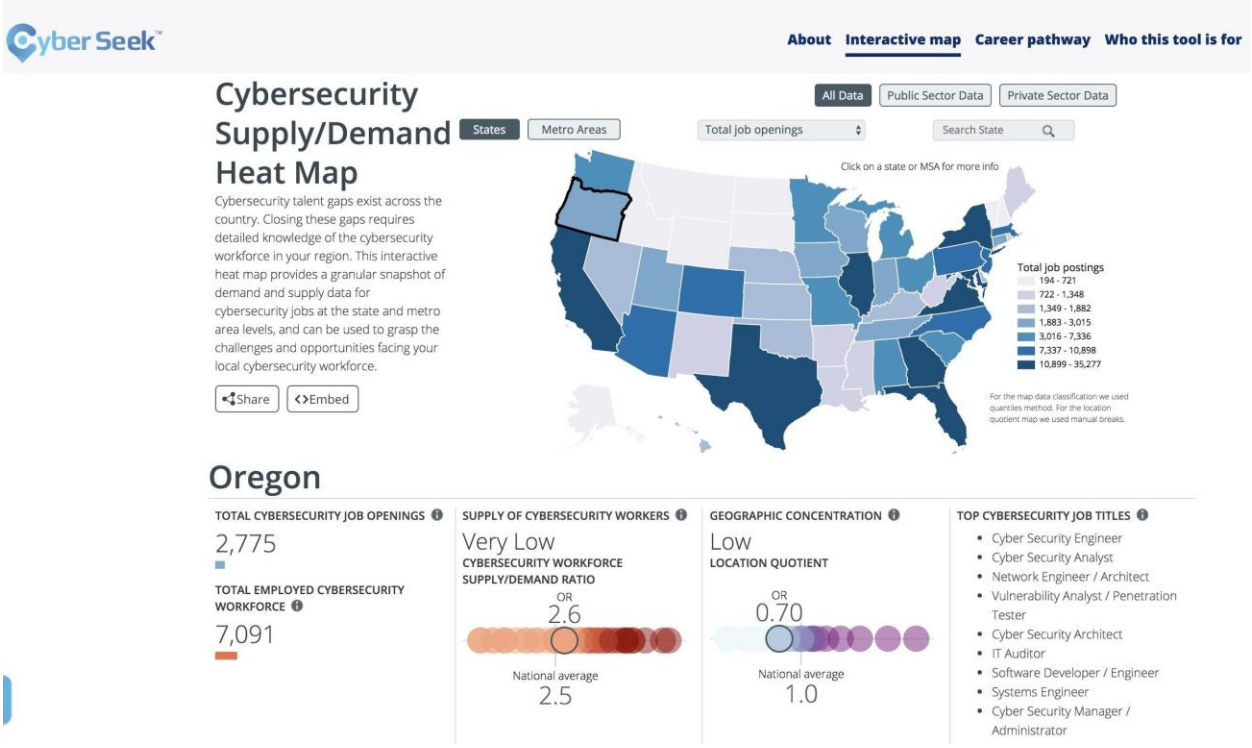

Fig. 1: Cybersecurity Supply / Demand Heat Map

I. improve educational attainment in the region and state;

By offering education locally for students interested in Cybersecurity, Oregon Tech will deliver geographically accessible courses so that students can obtain their security degrees locally. There are current statewide initiatives, Cyber Oregon being one of those initiatives to improve education and help attain a qualified workforce in Cybersecurity.

II. respond effectively to social, economic, and environmental challenges and opportunities; and

Oregon Tech will offer the B.S. Cybersecurity as an on campus offering initially in both Portland – Metro and Klamath Falls campus locations. The fall of 2021 will be the launch of the B.S. Cybersecurity through Oregon Tech Online. Providing the Cybersecurity degree at all locations will limit geographic and social barriers to pursue this degree.

Oregon Tech developed the B.S. Cybersecurity with transferability in mind to help limit economic constraints on both the student and university. Students that transfer from a community college with an AAS in Cybersecurity or degree in business, computer information systems, computer support or other like disciplines will be able to transfer general education and core courses for many of those majors.

While pursuing the B.S. Cybersecurity students can transfer within Oregon Techs management department programs with ease as all the programs support the same common business core outcomes and courses.

III. address civic and cultural demands of citizenship.

Educational attainment depends on access, and providing the program in urban, rural and online formats maximizes the opportunities statewide for students to engage in the program. Cybersecurity is also an interesting field and can be attractive to a wide variety of students: those interested in deeply technical subjects as well as those who are more compelled by the social, ethical, policy and risk analysis aspects of the field. Cybersecurity is a viable "second option" for someone who has an existing degree in a non-technical field but aspires for better/different career opportunities.

One of the biggest social and cultural challenges we face in cybersecurity is how we address threats to our privacy and security while preserving liberty. Cybersecurity affects everyone and depends on the actions of every individual. As such, broadening societal understanding of the technical and social mechanisms by which attacks occur can inoculate us to some of the threats. Cybersecurity is also an exercise in escalation: as we develop better tools to thwart attacks, attackers become savvier. The technical and ethical challenges in the field will expand, not diminish, and there is urgent demand for higher education to provide education to help with the solution. There is space in Oregon for multiple institutions to provide cybersecurity education, which has quite different technical areas of focus that could be supported through complementary programs.

Ongoing dialogue about ethics and various approaches to cybersecurity are integrated throughout the program and are essential to the development of a full professional in the field.

3 Accreditation

a. Accrediting body or professional society that has established standards in the area in which the program lies, if applicable.

IACBE Accreditation: This degree program has been designed to meet the International Accreditation Council for Business Education (IACBE). All Oregon Tech business programs are currently accredited through IACBE (IACBE Accreditation). This accreditation is both mission-driven and outcomes-based in support of quality business education. All accreditation reviews require an independent, external evaluation of the program.

CAE-CDE Designation: In addition, this degree has been designed to meet the requirements of the National Centers of Academic Excellence in Cyber Defense program (CAD-CD) that is jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). The accreditation designation for four-year baccalaureate education is CAE-CDE. The

NSA/DHS offers designations for education (CAE-CDE), research (CAE-CDR), and community colleges (CAE-2Y). If so designated, Oregon Tech would become the first university bachelor's program to be designated in Oregon and one of only three in the Pacific Northwest (List of Designated Programs, 2018). There are currently two community colleges that have been designated as CAE-2Y.

b. Ability of the program to meet professional accreditation standards. If the program does not or cannot meet those standards, the proposal should identify the area(s) in which it is deficient and indicate steps needed to qualify the program for accreditation and date by which it would be expected to be fully accredited.

IACBE Accreditation: The proposed cybersecurity degree incorporates the Management Department's core business education curriculum. The core business program and its corresponding student learning outcomes are included as part of this proposal. This Management Department's core curriculum is currently accredited by IACBE for all other business programs at Oregon Tech.

CAE-CDE Designation: The proposed curriculum has been designed to meet the 2019 requirements which include: 1. Regional accreditation as outlined by the Department of Education, 2. Mapping of the curriculum to the four-year core Knowledge Units (KUs) plus five required options, 3. Demonstration of program in the following areas - outreach and collaboration, a robust and active cyber defense academic program, multidisciplinary efforts, practice of cyber defense at the institution, and among faculty and students.

c. If the proposed program is a graduate program in which the institution offers an undergraduate program, proposal should identify whether or not the undergraduate program is accredited and, if not, what would be required to qualify it for accreditation.

Not applicable.

d. If accreditation is a goal, the proposal should identify the steps being taken to achieve accreditation. If the program is not seeking accreditation, the proposal should indicate why it is not.

IACBE Accreditation: Since Oregon Tech's business programs are currently accredited by IACBE, the cybersecurity program will likewise follow IACBE's process to accredit new programs. The following steps will be completed for accreditation once the program has at least one set of graduates: 1. File an application for new program accreditation, 2. Submit an outcomes assessment plan that addresses student learning outcomes, 3. Prepare a new program self-study, 4. If applicable, undergo a site-visit, 5. Be reviewed by the IACBE Board of Commissioners.

CAE-CDE Designation: To become a designated CAE-CDE program the following steps will be taken: 1. File an application for new program accreditation that also includes a letter of intent and a new applicant checklist, 2. Work with a CAE program mentor to receive an endorsement once the application has been reviewed to have met the curriculum requirements. 3. Become a designated program upon receiving at least three independent reviews of our application by designated subject matter experts.

4 Need

a. Anticipated fall term headcount and FTE enrollment over each of the next five years.

The growing demand for Cybersecurity professionals has educational institutions ramping up to develop and offer cybersecurity focused curriculum and degree programs. Currently, Chemeketa, Lane, Mount Hood, and Portland Community Colleges have or are working on associate and transfer degree programs in or related to Cybersecurity. The relationships that Oregon Tech builds and establishes with these institutions helps to establish a pipeline of students for the Cybersecurity program.

To capture potential enrollment for the Cybersecurity degree, student data research suggests following student pipelines from high school and community college programs as Oregon Tech's enrollment is primarily made up of transfer students. Fall 2017 numbers for the institution indicate there were ~826 transfer students in the college of ETM of which ~776 were in STEM programs. At Oregon Tech, 69% of enrollees in STEM programs are computing majors, resulting in 535 students based on 2017 data. The Management department captured ~33% enrollment of all computing programs at Oregon Tech which is 176 students (Institutional Research, 2017).

Based on community college data published by Oregon.gov, ~12,000 community college students complete a 2-year program have been relatively flat since 2011-2012. 26% of graduating community college students continue to a four-year institution (Roach, 2009). Nationally, 48% of college students pursue a STEM degree (Chen, 2013). Using the figures published by Chen and Roach, an estimated 1,497 students go on to pursue STEM degrees each year in the state of Oregon, upon completing their community college work.

According to the Office of Institutional Research at Oregon Tech, 76% of students are Oregon residents. Of the Management Department's computing students, ~134 are Oregon residents. Oregon tech had 2360 new students Fall 2017. If the number of new students continues to increase by 10% a year to reach the university's 5-year goal, the university would have 3540 new students in 5 years. Computing programs in the Management Department capture ~7.5% of incoming new students (176/2360).

The department's best guess, based on advising students, is that 20% (26) of current on campus computing students in the Management Department will choose cybersecurity and will transfer into Cybersecurity from the Information Technology program. The first-year projections include the 20% student transfer count and a 15% growth in computing programs within the Management Department. There is potential for an increase

in students coming into the department computing programs of up to 25% for the cybersecurity program for the second and third year after program launch. Enrollment will then average out to the institutional goal of 10% growth per year. There will be additional growth in 2021 with the launch of the online program. Projections are calculated using current online enrollment, 60 students (Fall 2017 online enrollment), and Oregon Tech's anticipated growth rate of 10% and an additional 10% growth from marketing efforts for the new cyber degree program. 20% (18) of initial online numbers will be projected Cybersecurity enrollment which are transfers from other computing programs. After 2021-2022 growth is projected at 10% per year across all modalities.

	2019-20	**2020-21**	**2021-22**	**2022-23**	**2023-24**
Campus FTE	45	56	71	78	85
Online	0	0	21	25	30

Table 1: Estimated 5-Year Enrollment across all locations
**current on campus IT program enrollment is 130 as of Fall 2017*

b. Expected degrees produced over the next five years.

6- year graduation rates published by the state of Oregon is ~63%.

	2021-22	**2022-23**	**2023-24**	**2024-25**	**2025-26**
FTE	28	35	44	49	66

Table 2: Estimated Annual Graduations across all locations

c. Characteristics of students to be served (resident/nonresident/international; traditional/nontraditional; full-time/part-time, etc.).

The Cyber degree is designed to serve full- or part-time students. It is anticipated that the students attending Oregon Tech, Klamath Falls campus, will be full-time students. Students attending Portland-Metro and online will include both full- and part-time students.

Currently there are no universities offering a specific 4-year baccalaureate-level degree in cybersecurity within the State of Oregon. Several of the universities in the state offer a B.S. in Computer Science or security certificates that can include elective coursework in some aspects of cybersecurity, however they are not exclusively focused on the applied practice of cybersecurity.

CIS programs from Chemeketa, Lane, Mount Hood, Clark, Umpqua, Rogue and Portland Community Colleges regularly feed into the B.S. in Information Technology program at Oregon Tech. Several of these schools either already have, or are actively working on, developing specific Cybersecurity programs, and have expressed high interest in developing articulation agreements, 2+2, or 3+2 transfer programs with Oregon Tech to provide a clear pathway for their students to earn a baccalaureate level degree.

d. Evidence of market demand.

Evidence of market need

The United States Homeland Security states,

"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

America needs well trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation. The Department of Homeland Security (DHS) is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders of tomorrow.

As greater priority is placed on strengthening cybersecurity, our nation is increasingly looking to higher education to produce skilled and capable cybersecurity professionals able to defend our networks and infrastructure. In response, DHS and The National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program, designating specific 2- and 4-year colleges and universities as top schools in Cyber Defense (CD). Schools are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field. CAE graduates help protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors."

The Bureau of Labor Statistics (BLS) represents Information Security Analyst growing at 28% over the next 8 years under the fastest growing occupations: 20 occupations with the highest percent change of employment between 2016-26. (Figure 2).

OCCUPATION	GROWTH RATE, 2016-26	2017 MEDIAN PAY
Solar photovoltaic installers	105%	$39,490 per year
Wind turbine service technicians	96%	$53,880 per year
Home health aides	47%	$23,210 per year
Personal care aides	39%	$23,100 per year
Physician assistants	37%	$104,860 per year
Nurse practitioners	36%	$103,880 per year
Statisticians	34%	$84,060 per year
Physical therapist assistants	31%	$57,430 per year
Software developers, applications	31%	$101,790 per year
Mathematicians	30%	$103,010 per year
Physical therapist aides	29%	$25,730 per year
Bicycle repairers	29%	$28,390 per year
Medical assistants	29%	$32,480 per year
Genetic counselors	29%	$77,480 per year
Occupational therapy assistants	29%	$59,310 per year
Information security analysts	28%	$95,510 per year
Physical therapists	28%	$86,850 per year
Operations research analysts	27%	$81,390 per year
Forest fire inspectors and prevention specialists	27%	$37,380 per year
Massage therapists	26%	$39,990 per year

Last Modification: Friday, April 13, 2018
Fig. 2: BLS Occupational Outlook Fastest Growing Occupations

The National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology (NIST) through the US Department of Commerce published findings that 1.8 million more cybersecurity professionals will be needed to fill the global shortage of positions by 2022; 64% of cybersecurity jobs will

require a bachelor's degree and 21 % graduate degrees. Additionally, computer and mathematical occupations will grow 13.5% in the next 8 years (Figure 3).

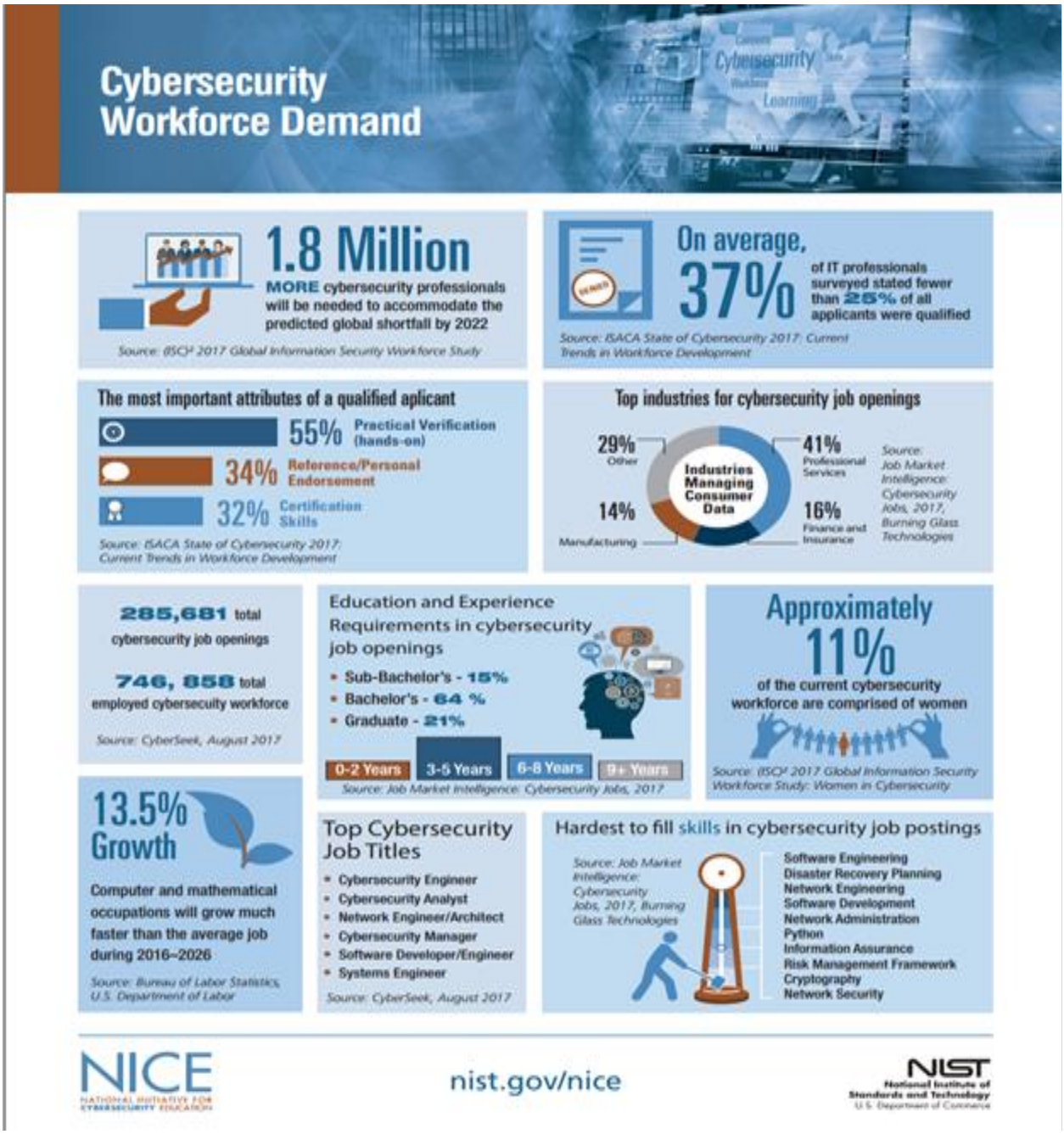

Fig. 3: nist.gov/nice Cybersecurity Workforce Demand

Presidio's President Waheed Choudhry is excited and wanting bring on Oregon Tech students as paid interns (See Appendix C, Item G).

e. If the program's location is shared with another similar Oregon public university program, the proposal should provide externally validated evidence of need (e.g., surveys, focus groups, documented requests, occupational/employment statistics and forecasts).

Not applicable.

f. Estimate the prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate. What are the expected career paths for students in this program?

As stated under section 4d, Market Demand, it is predicted that there will be a shortage of cybersecurity professionals by 2022. In addition to the shortage of professionals, there is a growing demand for cybersecurity positions. Entry-level positions include, but are not limited to, Cybersecurity Specialist/Technician, Cyber Crime Analyst/Investigator, Incident Analyst/Responder and IT Auditor. Mid-Level positions include but are not limited to Cybersecurity Analyst, Cybersecurity Consultant, and Penetration and Vulnerability Tester. Leading industries expressing a growing need for Cybersecurity professionals include Healthcare, social assistance, finance, insurance and retail.

Indeed.com reports Cybersecurity salaries in Oregon ranging from $55,000 to $82,000 (Figure 4).

Industry support Letters

Col. Jeff Smith "Oregon Air National Guard" Kingsley Field (See Appendix C, Item H).

Waheed Choudhry President "Presidio" (See Appendix C, Item G).

Cyber Security Salaries in Oregon

Salary estimated from 1,694 employees, users, and past and present job advertisements on Indeed in the past 36 months. Last updated: September 14, 2018

Location

Oregon

Information Design & Documentation	Average Salary	Salary Distribution
IT Security Specialist 5 salaries reported IT Security Specialist jobs in Oregon	**$29.57** per hour	Most Reported $7.25 – $23.55
Information Security Analyst 10 salaries reported Information Security Analyst jobs in Oregon	**$81,579** per year	$14,500 – $47,100
Intelligence Analyst 5 salaries reported Intelligence Analyst jobs in Oregon	**$78,435** per year	$14,500 – $47,100
Information Technology Specialist 7 salaries reported Information Technology Specialist jobs in Oregon	**$16.83** per hour	$7.25 – $23.55

Fig. 3:Indeed.com Cybersecurity Salaries, Oregon indeed

According to Indeed.com, average national entry level Cybersecurity salaries range from $74,000 to $106,000 (Figure 5).

Entry Level Cyber Security Salaries in the United States

Salary estimated from 10,852 employees, users, and past and present job advertisements on Indeed in the past 36 months. Last updated: September 18, 2018

Location

United States

Security & Public Safety	Average Salary	Salary Distribution
Security Consultant 723 salaries reported Security Consultant Jobs	**$74,153** per year	Most Reported $27,000 – $203,000

Information Design & Documentation	Average Salary	Salary Distribution
Information Security Analyst 1,809 salaries reported Information Security Analyst Jobs	**$79,841** per year	$27,000 – $203,000
IT Security Specialist 4,984 salaries reported IT Security Specialist Jobs	**$105,960** per year	$27,000 – $203,000

Fig. 5: Indeed.com Entry Level Cyber Security Salaries (National Data)

5 Outcomes and Quality Assessment

a. Expected learning outcomes of the program.

The B.S. in Cybersecurity is designed to produce graduates that will be ready to enter the workforce as entry-level cybersecurity practitioners, analysts, and penetration testers. Students will be exposed to the fundamentals of computer organization and architecture, operation systems, network routing and switching, and database management, along with specialized courses in cyber defense operations, vulnerability scanning and reporting, cyber incident response, and information system risk management.

In addition to a strong technical background, students will gain professional skills needed to be successful in a diverse cybersecurity workforce. This is accomplished by incorporating the Management Department's core curriculum into the program's curriculum map.

Management Department Student Learning Outcomes:

1. Communicate the major concepts in the functional areas of accounting, marketing, finance, information technology and management.
2. Describe the legal, social, ethical, and economic environments of business in an internal/external (global) context.
3. Solve organization problems, individually and/or in teams, using quantitative, qualitative, and technology-enhanced approaches.
4. Demonstrate professional communication and behavior.
5. Apply knowledge of business concepts and functions in an integrated manner.

Students graduating with a B.S. in Cybersecurity from Oregon Tech will also demonstrate proficiency in each of Oregon Tech's Essential Student Learning Outcomes (ESLOs), including the ability to:

1. Communicate effectively orally and in writing
2. Engage in a process of inquiry and analysis
3. Make and defend reasonable ethical judgments
4. Collaborate effectively in teams or groups
5. Demonstrate quantitative literacy
6. Explore diverse perspectives

In addition to institutional and departmental student learning outcomes, students earning the B.S. in Cybersecurity will also be able to demonstrate proficiency in the following Program Student Learning Outcomes (PSLOs):

i. Describe the tactics, techniques, and procedures used throughout the vulnerability assessment process.
ii. Evaluate risk in information systems and apply mitigation techniques to reduce impact to business operations.
iii. Perform information system vulnerability scanning and report findings.
iv. Identify information system exploits and apply proper incident response.

Program Student Learning Outcomes (PSLOs)	Assessment Schedule		
Cyber Security	Fall	Winter	Spring
Describe the tactics, techniques, and procedures used throughout the vulnerability assessment process	CYB 301(KF and PM)		MIS 498 (KF and PM)
Evaluate risk in information systems and apply mitigation techniques to reduce impact to business operations.	CYB 411 (KF and PM)		MIS 498 (KF and PM)
Perform information system vulnerability scanning and report findings.	CYB 411 (KF and PM)		MIS 498 (KF and PM)
Identify information system exploits and apply proper incident response.		CYB 302 (KF and PM)	MIS 498 (KF and PM)

**Klamath Falls (KF), Portland Metro (PM)*

Table 3: Program Student Learning Outcomes Assessment Calendar

b. Methods by which the learning outcomes will be assessed and used to improve curriculum and instruction.

Departmental outcomes are assessed using both direct and indirect methods.

Indirect measures used by the Management Department include a student exit survey, administered to all Management Department majors.

Programmatic student learning outcomes are measured within courses directly related to the specific outcome. Measures include examinations, papers, and case analyses. Program Student Learning Outcomes (PSLOs) will be assessed primarily in the required one-year capstone experience. In addition, student work performance will be regularly evaluated with respect to the PSLOs using a standard rubric.

Prospects for graduate success are very strong. Oregon Tech's focused curricula and reputation have led to high employment and graduate school success for Oregon Tech Management Department graduates over the past 15 years. Similar to other Management Department degree offerings, the Cybersecurity degree incorporates well-developed, existing courses taught by seasoned faculty members.

Oregon Tech Essential Student Learning Outcomes (ESLOs) will be evaluated based on standard university processes.

c. Nature and level of research and/or scholarly work expected of program faculty; indicators of success in those areas.

The primary focus for faculty in this program will be in maintaining high levels of professional development. Cybersecurity is a rapidly changing discipline that requires a significant amount of time and effort to maintain an appropriate level of expertise. Faculty will be expected to participate in continuing education activities.

6 Program Integration and Collaboration

a. Closely related programs in this or other Oregon colleges and universities.

Currently there are no universities offering a specific 4-year baccalaureate-level degree in cybersecurity within the State of Oregon. The current offerings are stated below:

Portland State University
- Graduate Computer Security Certificate

Portland Community College
- Certificate in Cybersecurity Fundamentals
- Associates degree with CAE2Y accreditation

Mount Hood Community College
- Associates degree with CAE2Y accreditation

Chemeketa Community College
- AAS Systems Administration and Network Security

Lane Community College
- Career Pathway Certificate in Computer Network Security

Oregon State University
- Bachelor's Degree in computer science with an Applied Option in Security

George Fox University
- Bachelor's Degree in computer science with a concentration in Cyber Security

University of Oregon
- Cyber Research Center with CAE-R accreditation

b. Ways in which the program complements other similar programs in other Oregon institutions and other related programs at this institution. Proposal should identify the potential for collaboration.

The B.S. Cybersecurity degree is housed within the Management Department at Oregon Tech. All students in the Cybersecurity program will complete the management core which will provide foundational knowledge for students choosing to pursue MBA programs at any of the degree granting institutions in the state of Oregon. Students in the Cybersecurity degree also have the foundational knowledge necessary to pursue master's degrees in computer science related degrees.

Incoming students can enter the Cybersecurity degree easily from several different associate degree programs around the state. Degrees in Computer Information Systems, Business, and Computer Science related degrees will transfer both general education and lower-division programmatic courses into the degree.

The expectation is to pursue articulation agreements and degree pathways with community colleges such as are is in place now for degrees within the Management Department.

Oregon tech will look to partner and collaborate with community colleges to develop degree pathways as well as with the Oregon Air National Guard to identify potential education pathways for cyberspace operations Airmen (See Appendix C, Item H).

c. If applicable, proposal should state why this program may not be collaborating with existing similar programs.

Not applicable.

d. Potential impacts on other programs.

Introducing the degree in Cybersecurity will excite a number of students and there is a possibility that some students will switch majors. The primary program that might be affected is the Information Technology program which is housed within the Management Department resulting in internal cannibalization between the degrees in the short term.

Computer Systems Engineering Technology might have some students switch to Cybersecurity. Todd Breedlove, Department Chair, has been consulted, is aware of the possibility, and has provided support (See Appendix C, Item E).

The general education departments have all been consulted and are aware of potential increases in select courses within their curriculum. Dept. Chairs Mark Neupert, Dan Peterson, and Tiernan Fogarty have all provided support (See Appendix C, Items B, C and F).

The business programs are also aware of the potential increases or decreases in enrollment. Dept. Chairs Maureen Sevigny and Sharon Beaudry have all been consulted (See Appendix C, Item D)

7 Financial Sustainability

a. Business plan for the program that anticipates and provides for its longterm financial viability, addressing anticipated sources of funds, the ability to recruit and retain faculty, and plans for assuring adequate library support over the long term.

In support of our B.S. in Cybersecurity, we have higher education faculty and obtained the needed lab equipment for our campuses.

To recruit and retain faculty, we will follow established university recruiting processes. With regard to retaining faculty, we will provide professional development opportunities and industry connections. As for library services: We have librarian support embedded within our Blackboard course shells. We collaborate with our library for digital services and research support. Our subscription to Safari Books provides students with access to a wide array of texts as well.

The proposed budget for the BS in cybersecurity has a breakeven point in FY 3 (AY 4) and returned profit at EOY of $406,559.

b. Plans for development and maintenance of unique resources (buildings, laboratories, technology) necessary to offer a quality program in this field.

The department of management proposes three potential lab configurations.

(1.) On Premise + Public Cloud

Our ideal lab configuration offers direct hands-on experience with equipment onsite located within our own datacenter and can scale out to the public cloud (primarily Amazon Web Services via AWS Educate partnership). This configuration positions us best and provides visibility and presence. The On Premise component has the cost of maintenance and related software subscriptions on the existing hardware that was acquired with the initial cybersecurity grant. For the Public Cloud portion, we can tie direct student lab costs to the student taking the course using a model similar to a tech fee.

(2.) Public Cloud

Our second preference is a Public Cloud only option. In this configuration we solely utilize Public Cloud Infrastructure. We can accomplish this offering via Amazon Web Services Educate partnership. Within this option, costs would be tied to student enrollment (i.e. we only need to provision the resources based on the number of students that we have enrolled). We can tie direct student lab costs to the student taking the course using a model similar to a tech fee (i.e. an "Extra Class / Course Fee").

(3.) On Premise

Our third preference is an on-premise lab. A lab which is solely on premise has some of the benefits outlined but is hindered by the inability to scale. This represents the highest overall cost in terms of capital outlay and maintenance costs.

Existing Equipment:

The equipment acquired through the initial cybersecurity grant belongs to the Management department and will be used in furtherance of the proposed Cybersecurity degree. This means we can take ownership of all equipment on the listing and repurpose to support the lab for the Cybersecurity degree.

Redundancy is important to any highly available IT environment. The cybersecurity grants provide enough equipment to separate and build mirrored lab environments at the Klamath Falls and Portland-Metro campuses. To achieve redundancy, each campus lab environment will serve as an offsite backup storage solution for the other campus. The result is an always-available lab environment and smart resourcing of existing equipment.

Detail of On Premise:

The numbers resulting from the cybersecurity grant show $659,059 as the starting figure for capital outlay for On Premise infrastructure. Equipment lifecycle replacement costs are calculated at 20% and 30% to show flexibility when finalizing the budget. It is important to note the 20% calculation will result in older lab equipment, driving higher equipment failure risk as equipment age increases. The replacement costs are also shown with 3- and 5-year lifecycles. The 3-year lifecycle is ideal to minimize risk in equipment failures and keeping current technologies in the lab environment. These calculations are in line with industry equipment management best-practices.

Starting at $659,059, the 20% equipment replacement costs calculate to $131,811. An equipment refresh rate of 3 years at 20% calculates to $43,937 annually. An equipment refresh rate of 5 years at 20% calculates to $26,362 annually. The 30% equipment replacement costs calculates to $197,717. An equipment refresh rate of 3 years at 30% calculates to $65,905 annually. An equipment refresh rate of 5 years at 30% calculates to $39,543 annually.

Detail of Public Cloud:

The costs for Public Cloud services should be able to be contained within an extra class fee per class per student participating within the Cybersecurity degree. By having an "extra class fee" of $ 100, students will have the available resource budget on Amazon AWS to have on average 3 virtual machines for their labs running over the course of 10 weeks with the necessary utilization in terms of compute and storage hours.

To remain flexible and budget conscious we will work with our program directors, dean and related we will work diligently to bring cost under control and long term sustainable.

This equipment can also be leveraged by IT and HI degrees. Cross-utilization of laboratory equipment between Cybersecurity, IT, and HI programs results in high-utilization of existing resources. The programs together across all modalities the total students served would be approximately 250 (Cybersecurity, IT, HI, etc.).

c. Targeted student/faculty ratio (student FTE divided by faculty FTE).

The target student/faculty ratio is 20:1.

d. Resources to be devoted to student recruitment.

Recruiting efforts include working with the Office of Academic Partnerships to develop articulation agreements and OIT publications, as well as with the Offices of Strategic Enrollment Management and Admissions. It is anticipated that no resources will be devoted exclusively to recruitment as it will become part of the larger Management Department's recruiting efforts.

8 External Review

a. If the proposed program is a graduate level program, follow the guidelines provided in External Review of New Graduate Level Academic Programs in addition to completing all of the above information.

Not applicable.

APPENDIX

A. Approval to Proceed

B. Summary for OIT Curriculum Planning Commission

- **1.** New Courses
- **2.** Program Narrative
- **3.** Curriculum Map
- **4.** General Education Requirements

C. Documentation of communication

D. References

Appendix A: Approval to Proceed

Oregon TECH

Curriculum Proposal Cover Sheet
for New Degrees, New Degree Options, Significant Program Revisions, etc.

Approval to Proceed / Final Approval

Department: Management Program: B.S. Cybersecurity

Submitter's Name: Kris Rosenberg Phone: 503-821-1309 Email: kris.rosenberg@oit.edu

Proposal submission date: October 28th, 2016

Implementation requested for academic year: 2018-19 (2017-18 if possible)

Type of curriculum proposal:

- ☑ New degree
- ☐ New degree option
- ☐ Significant program revision
- ☐ Curriculum change requiring additional funding, facilities or staff
- ☐ Minor
- ☐ Certificate
- ☐ Specialization
- ☐ Emphasis
- ☐ Other

Abstract of the proposed change:

There is a undenialbe need for for cybersecurity professionals with knowledge and skils in the technologies, processes and practices needed to protect networks, computers, programs and data from attack, damage or unauthorized access. Cybersecurity represents a new unique and specialized profession that is separate from traditional business, IT and engineering disciplines that combines skill sets from these disciplines along with highly specialized knowledge and skills that are unique to Cybersecurity. Therefore it is reccomended that a new B.S. in Cybersecurity degree be devloped

Signatures below constitute **Approval to Proceed** in the curriculum proposal process:

Date: 11/2/16 Approved by: Maureen Dempsey, Department Chair

Date: 11/2/16 Approved by: Jean Nugent, Dean

Date: 11/4/16 Approved by: Rob Mayer, Provost

Signatures below constitute **Final Approval** of this proposal:

Date: 1-3-18 Approved by: Hallie Neupert, Department Chair

Date: 24 Jan 18 Approved by: , Director of Assessment

Date: 1-24-18 Approved by: Jean Nugent, Dean

Date: Approved by: , CPC

Date: Approved by: , Provost

Appendix B: Summary for OIT Curriculum Planning Commission

1. New Courses

Class Number and Name	Cr.
MIS 240 Linux OS	3-3-4
MIS 285 Python Programming	3-3-4
MIS 365 Cloud Computing	3-3-4
CYB 201 Cyber Security Fundamentals	3-0-3
CYB 301 Hacker Tools and Techniques	3-3-4
CYB 302 System Defense and Incident Response	3-3-4
CYB 303 Security Operations and Analysis	3-3-4
CYB 351 Network Security	3-3-4
CYB 411 Managing Risk and Information Systems	3-0-3
	34

2. Program Narrative

Degree Offered

Bachelor of Science in Cyber Security

This program offers a BS in Cyber Security to students who interests lie in business, computer information systems and goal of securing business assets.

Student Preparation and Admissions

Students must meet the standard OIT admissions requirements. Transfer students must arrange for official transcripts from each college and university attended to be sent to OIT.

3. Curriculum Map

BS in Cyber Security			
	NEW CURRICULUM		
Prerequisite	**Freshman Year - Fall**		
Math 100	MATH 111	College Algebra	4
	SPE 111	Public Speaking	3
WRI 115	WRI 121	English Composition	3
		Lab Science Elective	4
		TOTAL:	14
	Freshman Year - Winter		
College Level Math	ECO 201	Principles of Microeconomics	3
	MIS 102	Spreadsheet Lab	1
	MIS 145	Introduction to PC Hardware/Software	4
WRI 121	WRI 122	Argumentative Writing	3
MATH 111	MATH 112	Trigonometry	4
		TOTAL:	15
	Freshman Year - Spring		
	BUS 215	Principles of Management	3
MIS 145	MIS 251	Networking I	4
	MIS 275	Introduction to Relational Database	3
Math 111	MIS 285	Python Programming	4
		TOTAL:	14
	Sophomore Year - Fall		
Math 100	ACC 201	Principles of Accounting I	4
Math 111	MIS 118	Introduction to Programming in C#	4
MIS 145	MIS 273	Systems Administration I	4
WRI 122 and SPE 111	WRI 227	Technical Report Writing	3
		TOTAL:	15
	Sophomore Year - Winter		
	BUS 226	Business Law	3

MATH 111	MATH 361	Statistical Methods I	4
MIS 118 and MIS 275	MIS 218	Database Programming	4
	CYB 201	Cyber Security Fundamentals	3
WRI 227	PHIL 331	Ethics in the Professions	3
	or		
WRI 122 and 3 cr. Hum Electives	PHIL 342	Business Ethics	3
		TOTAL:	17
	Sophomore Year - Spring		
ACC 201	ACC 203	Principles of Managerial Accounting	4
MIS 145	MIS 240	Intro to Linux OS	4
BUS 215 or BUS 317	MGT 335	Project Management	3
College Level Math	ECO 202	Principles of Macroeconomics	3
SPE 111	SPE 321	Small Group and Team Communication	3
		TOTAL:	17
	Junior Year - Fall		
ACC 203	ACC 325	Finance	4
MIS 251	MIS 351	Routing and Switching I	4
WRI 121	MIS 311	Introduction to Systems Analysis	3
		Humanities Elective	3
CYB 201 and MIS 285 and WRI 227	CYB 301	Hacker Tools and Techniques	4
		TOTAL:	18
	Junior Year - Winter		
MIS 275 and MIS 311	MIS 312	Systems Analysis I	4
MIS 118 and MIS 275	MIS 341	Relational Database Design I	4
WRI 227	WRI 350	Documentation Writing	3
	or		
WRI 227	WRI 327	Advanced Tech Writing	3
MATH 361 and MIS 113 or MIS 275	MIS 334	Business Analytics	3
CYB 301 and MIS 351	CYB 302	System Defenses and Incident Response	4
		TOTAL:	18
	Junior Year - Spring		
	BUS 223	Marketing I	3

MIS 218, MIS 312, MIS 341	MIS 322	Systems Analysis II	4
MIS 312 and MGT 335	MIS 495	Senior Project Selection	1
CYB 301 and SPE 321	CYB 303	Security Operations and Analysis	4
CYB 201 and MIS 351	CYB 351	Network Security	4
		TOTAL:	16
	Senior Year - Fall		
MIS 251 and MIS 273	MIS 365	Cloud Computing	4
MIS 495 and MIS 322	MIS 496	Senior Project Mgmt	3
BUS 215 or BUS 304 and MIS 206 or MIS 311	CYB 411	Managing Risk in Information Systems	3
BUS 215, BUS 304, BUS 317	MGT 321	Operations Management	3
		TOTAL:	13
	Senior Year - Winter		
SPE 111 and WRI 122	BUS 356	Business Presentations	4
MIS 496	MIS 497	Senior Project I	3
Junior Standing or Instructor's Consent	PSY 347	Organizational Behavior	3
BUS 215, BUS 304, BUS 317	BUS 349	Human Resource Mgmt	3
		TOTAL:	13
	Senior Year - Spring		
MIS 497	MIS 498	Senior Project II	3
ACC 203 and WRI 227	BUS 478	Strategic Management	3
WRI 122	ANTH 452	Globalization	3
		Humanities Elective	3
		TOTAL:	12
		Degree Total	182

4. **General Education Requirements**

The BS in Cybersecurity will meet the institution's policy for general education requirements as follows. Please note that on November 20th, 2012 the management department received an exemption to the 36/45 general education rule by the registrar (See Appendix C, Item A).

General Education Requirements Summary		
Communication: 18 Credits		
SPE 111	Public Speaking	3
SPE 321	Small Groups and Teams	3
WRI 121	English Composition I	3
WRI 122	English Composition II	3
WRI 227	Tech Report Writing	3
WRI 350	Documentation Writing	3
		18
Humanities: 9 Credits		
PHIL 331 or 342	Ethics in the Professions or Business Ethics	3
	Humanities Electives	6
		9
Math / Science: 12 Credits		
MATH 111	College Algebra	4
MATH 112	Trigonometry	4
MATH 361	Statistical Methods	4
		12
Lab Science: 4 Credits		
	Lab Science Elective	4
		4

Social Science: 12 Credits		
ECO 201	Macroeconomics	3
ECO 202	Microeconomics	3
	ANTH 452 or HIST 452	3
PSY 347	Organization Behavior	3
		12
Upper Division: 60 Credits		
MIS 311	Introduction to Systems Analysis	3
MIS 312	Systems Analysis I	4
MIS 322	Systems Analysis II	4
MIS 341	Relational Database Design I	4
MIS 334	Business Analytics	4
MIS 351	Routing and Switching I	4
MIS 495	Sr. Project Selection	1
MIS 496	Sr. Project Management	3
MIS 497	Sr. Project I	3
MIS 498	Sr. Project II	3
CYB 301	Hacker Tools and Techniques	4
CYB 303	Security Operations and Analysis	4
CYB 351	Network Security	4
CYB 411	Managing Risk in Information Systems	3
MGT 321	Operations Management	3
MGT 335	Project Management	3
BUS 349	Human Resources Management	3
BUS 356	Business Presentations	3
		60

Appendix C: Documentation of Communication

a. Exemption of the 36/45 requirement

MEMORANDUM

OFFICE OF THE REGISTRAR

TO: Marla Miller

FROM: Wendy Ivie

DATE: Tuesday, November 20, 2012

SUBJECT: Management Department Programs – Math/Science/Social Science Requirement

---

Beginning with the 2012-13 catalog year, all Bachelor of Science degrees in the Management Department are not required to meet the umbrella requirement of 36 Math/Science credits or 45 Math/Science/Social Science credits. In the 2012-13 curriculum maps, all 'Math/Science/Social Science Electives' will be replaced with 'General Electives' in the Bachelor of Science degrees listed (note that all degrees are still required to complete at least 12 credits of Social Science):

Allied Health Management
Information Technology, Accounting Option
Information Technology, Applications Development Option
Information Technology, Business/Systems Analysis Option
Information Technology, Health Informatics Option
Management, Accounting Option
Management, Entrepreneurship/Small Business Management Option
Management, Marketing Option
Operations Management

In order for the 36/45 requirement to be waived for students following earlier catalog curriculums, a Course Substitution form will need to be submitted to the Registrar's Office.

Regards,

Wendy Ivie

Wendy Ivie
University Registrar

b. Letter of Support Math Department

From: Tiernan Fogarty
To: Jeff Dickson
Subject: RE: Degree Support
Date: Thursday, September 20, 2018 2:31:02 PM

Hi Jeff,

You bet! This is great. Good luck with the new program.

Thanks, Tiernan

From: Jeff Dickson
Sent: Thursday, September 20, 2018 1:36 PM
To: Tiernan Fogarty <Tiernan.Fogarty@oit.edu>
Subject: Degree Support

Hi Tiernan,

The department of management is proposing a major in Cyber Security. The program is adding MATH 111, 112 and 361.

The projected enrollment is:

20 in wilsonville and 15 klamath year 1 and an aggressive growth of 25% year 2 so 25 in wilsonville and 18 in klamath. There may be some also shifting out of IT into Cyber so they might not all be new students. Yes I made the adjustment for HIST in WLV thanks.

Can the math department support this enrollment growth?

Thanks,

Jeff Dickson
Associate Professor
Program Director, Health Informatics
Program Director, Information Technology

Oregon TECH

3201 Campus Drive
Mailstop: OW 143
Klamath Falls, Oregon 97601

Phone: 541-885-1857

c. Letter of Support Humanities Department

From: Mark Neupert
To: Jeff Dickson
Subject: Re: Departmental Support for Cyber Security
Date: Thursday, September 20, 2018 11:51:54 AM

Hi Jeff, HSS can support this requirement.

Cheers, Mark

From: Jeff Dickson
Sent: Thursday, September 20, 2018 8:49:56 PM
To: Mark Neupert
Subject: Re: Departmental Support for Cyber Security

Hi Mark,

20 in wilsonville and 15 klamath year 1 and an aggressive growth of 25% year 2 so 25 in wilsonville and 18 in klamath. There may be some also shifting out of IT into Cyber so they might not all be new students. Yes I made the adjustment for HIST in WLV thanks.

Jeff

Sent from my iPhone

On Sep 20, 2018, at 11:40 AM, Mark Neupert <Mark.Neupert@oit.edu> wrote:

> Hi Jeff, how many students? Location? On the ground in odd we only offering the Hist version.
> M
>
> ---
>
> **From:** Jeff Dickson
> **Sent:** Thursday, September 20, 2018 7:32:55 PM
> **To:** Mark Neupert
> **Cc:** Sharon Beaudry; Hallie Neupert; Maureen Sevigny
> **Subject:** Departmental Support for Cyber Security
>
> Hi Mark,
>
> The Management department is producing a proposal for a BS in Cyber Security. There are some prescribed courses from your department and we would like your departments support to offer the following courses. The BS in Cyber Security will be initially offered in Wilsonville and Klamath Falls and the courses we are needing are ANTH 452, PHIL 342 and PSY 201.
>
> Thank you,
>
> Jeff Dickson

d. Letter of Support Department of Management

From: Sharon Beaudry
To: Jeff Dickson; Hallie Neupert; Maureen Sevigny
Subject: Re: Program Support
Date: Thursday, September 20, 2018 10:57:36 AM

Hi,
In Klamath Falls we can handle the additional students. From my understanding the Wilsonville business core courses are not full, therefore we would also be able to handle those as well.

Sharon Beaudry, JD, SPHR
Associate Professor & Acting Department Chair
Business Management
541.885.1575 | sharon.beaudry@oit.edu
Oregon TECH
Tech-Infused Business Degrees
Webpage
Facebook

From: Jeff Dickson
Sent: Thursday, September 20, 2018 10:34:46 AM
To: Sharon Beaudry; Hallie Neupert; Maureen Sevigny
Subject: Program Support

Sharon, Hallie and Maureen,

As you know we are preparing the proposal for the Cyber Security degree. The proposed curriculum includes the Management core courses and will be needed in both Klamath Falls and Wilsonville campus. Will the BUS programs be able to handle the additional capacity and support the Cyber Degree?

Thanks,

Jeff Dickson
Associate Professor
Program Director, Health Informatics
Program Director, Information Technology

Oregon TECH

3201 Campus Drive
Mailstop: OW 143
Klamath Falls, Oregon 97601

Phone: 541-885-1857

e. Letter of Support Computer Systems Engineering

From: Todd Breedlove
To: Jeff Dickson
Subject: Re: CSET Support for Cyber Security
Date: Saturday, September 22, 2018 11:29:25 AM

Jeff,

We in CSET realize that there may be some shifting of students between our majors. However, it is our belief and advice to all of our students to go with what they love. If that is the cyber security degree, good for them.

I do look forward to working with you to add options for all of our students and opportunities for our departments to collaborate. Initiatives such as minors or concurrent degree options may be just some of the added possibilities.

As it moves forward, let's try to minimize the duplication of effort and course content. We have enough of that already.

Todd

Get Outlook for Android

From: Jeff Dickson
Sent: Saturday, September 22, 2018 10:11:52 AM
To: Todd Breedlove
Subject: CSET Support for Cyber Security

Todd,

We are working to revise the cybersecurity proposal. I would like to get your support for the possibility of future collaboration and options for the cyber security program that align with your department. While I do not have any figures to determine what type of internal conversion we might have with students. I need your recognition that there might be some CSET students that convert over to the cyber security program. Our deadline for this degree proposal is to be on Kuleks desk by Wednesday.

Thanks,

Jeff Dickson
Associate Professor
Program Director, Health Informatics
Program Director, Information Technology

Oregon TECH

3201 Campus Drive

f. Letter of Support Communication Department

Hi Jeff,

After discussing your proposal with the faculty in my department it was determined that your proposal will have no effect on WRI 121, WRI 122, SPE 111 or SPE 321. However, because we offer one, maybe two sections (depending on need) of WRI350 a year, if the cyber security degree was more flexible in the upper division writing requirement by considering one or two more possible upper division writing options (WRI 327 for example), students would have greater ability to take the WRI classes and complete without having to wait for WRI 350. Let me know if you have any questions about my feedback.

Regards,

Dan

From: Jeff Dickson
Sent: Thursday, September 20, 2018 1:37 PM
To: Dan Peterson <Dan.Peterson@oit.edu>
Subject: Program Support

Dan,

The management department is proposing a degree in cyber security. The courses utilized in this degree from your department is WRI 121, 122, 350, SPE 111 and SPE 321.

Project Enrollment is

20 in wilsonville and 15 klamath year 1 and an aggressive growth of 25% year 2 so 25 in wilsonville and 18 in klamath. There may be some also shifting out of IT into Cyber so they might not all be new students.

Can the communications department support this enrollment increase.

Jeff Dickson
Associate Professor
Program Director, Health Informatics
Program Director, Information Technology

Oregon TECH

3201 Campus Drive
Mailstop: OW 143
Klamath Falls, Oregon 97601

Phone: 541-885-1857

g. Internship Support from Presidio

From: Jim Jones2
Sent: Tuesday, September 25, 2018 1:30 PM
To: Jeff Hower <Jeff.Hower@oit.edu>; Lindy Stewart <Lindy.Stewart@oit.edu>; Sharon Beaudry <Sharon.Beaudry@oit.edu>; Dan Carrere <Dan.Carrere@oit.edu>; Tracey Coon <Tracey.Coon@oit.edu>
Subject: Cyber Security Internship.docx

Hello all!

Good news! I spoke to the president of Presidio, Waheed Choudhry, this AM and he is very interested in starting an internship program with us starting Fall 2019. The internship will be however many months we need, and it will be a paid internship at $15 per hour. Waheed would like some additional information about the internship, what is expected of the company, what are the outcomes etc. I attached a quick document that I stole from another organization online that offers internships. I think we can use this as a starting point to provide to the vendors for the internships.

Mr. Choudhry is very excited about this opportunity and has given tentative approval for up to three internships with their security and risk management team.

Please review the attached and edit. We can refine and dial it in before we send students there, for now we just need a good overview of what we expect the internship outcomes to be and what is expected of the company offering the internships.

I am sure y'all have worked with internships before but I found this useful:
https://www.huffingtonpost.com/maureen-dumas/building-a-framework-for-_b_2680394.html

Talk to you soon!

Jim R. Jones Ph.D.
AVP CIO
Information Technology Services
Oregon TECH

3201 Campus Drive, BH 123
Klamath Falls, OR 97601
541.885.1720 Office
541-205-8753 Cell

541.885.1919 Fax
www.oit.edu

"The secret of change is to focus all of your energy, not on fighting the old, but on building the new."
- Socrates

h. Industry support and potential collaboration with Oregon Air National Guard

From: Tracey Coon
To: Jeff Dickson; Lindy Stewart; Dan Carrere
Subject: Fwd: [Non-DoD Source] Oregon Tech & ORANG
Date: Wednesday, September 26, 2018 7:30:42 AM

External support from the Oregon Air National Guard!

Get Outlook for Android

From: Smith, Jeffrey S (Sled) Col USAF 173 FW (US)
Sent: Wednesday, September 26, 5:27 AM
Subject: Re: [Non-DoD Source] Oregon Tech & ORANG
To: Tracey Coon
Cc: Gelhardt, Scott A Capt USAF 173 FW (US), Shirar, Jennifer D SMSgt USAF 173 FW (US)

Tracey,

Thanks for reaching out. Yes, we are absolutely interested in continuing to build the strong partnership we have with Oregon Tech and we are excited to hear about your growing cybersecurity program.

Cybersecurity is an ever growing career field in the Air Force, and we are looking for talented individuals to fill those roles at Kingsley Field and elsewhere in the Oregon Air National Guard. We already have a talented roster of Oregon Tech graduates serving at Kingsley, and we look forward to adding more to the team!

All the best,

Jeff Smith, Col, ORANG
173 FW Commander
541-885-6173 (work)
541-331-8414 (cell)

Sent from my iPad

On Sep 22, 2018, at 11:57 AM, Tracey Coon <Tracey.Coon@oit.edu> wrote:

Hello Col Smith,

The purpose of this message is to gain your support on the proposed cybersecurity degree program here at Oregon Tech.

As you are aware, there is a large deficit between skilled cybersecurity professionals and the growing number of threats aimed at exploiting our information systems. Oregon Tech is

proposing a Bachelor of Science in Cybersecurity degree program that will help build a diverse cybersecurity workforce. Our program is built around the National Security Administration (NSA) and Department of Homeland Security (DHS) cybersecurity core knowledge units. In other words, our program will directly support the federal government's efforts in developing a cybersecurity workforce that is ready to defend our Nation's infrastructure. Furthermore, our program focuses on employers like you to ensure we are providing the best graduates of cybersecurity.

In this process, we seek external support from potential employers. Would you, on behalf of Oregon Air National Guard, be willing to hire recent graduates with a Bachelor of Science in Cybersecurity degree from Oregon Tech?

Finally, as we continue to build this program, are you willing to continue building a partnership between Oregon Tech and the Oregon Air National Guard to support our cybersecurity program?

On behalf of Oregon Tech and the Management Department, I truly appreciate all of your support in this community partnership. I look forward to our future discussions on cybersecurity, Oregon Tech, and the Oregon Air National Guard.

Best regards,

Tracey J. Coon
Assistant Professor, Information Technology

<image002.jpg>
3201 Campus Drive
Mailstop: OW 143
Klamath Falls, Oregon 97601

Phone: 541-885-0856
tracey.coon@oit.edu

Appendix D: References

Applied Cybersecurity Nice Requirements (n.d.). Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/one-pagers

Chen, X. (2013). STEM Attrition: College Students' Paths into and out of STEM Fields. Statistical Analysis Report. NCES 2014-001. National Center for Education Statistics.

Cyber Security Salaries, Oregon (n.d.) Retrieved from:https://www.indeed.com/salaries/Cyber-Security-Salaries,-Oregon

Cybersecurity Supply And Demand Heat Map. (n.d.). Retrieved from https://www.cyberseek.org/heatmap.html

Entry Level Cyber Security Salaries (n.d.). Retrieved from https://www.indeed.com/salaries/Entry-Level-Cyber-Security-Salaries

Executive Order 13800 Update Issue 1. (n.d.). Retrieved from https://www.us-cert.gov/eo13800/Issue-1

HECC D4A Data Mart. (2017). Total Degree and Certificate Completion. Retrieved from https://www.oregon.gov/highered/research/Documents/Student/CC-completion-history.pdf

HECC Office of Research and Data. (2017). University Student Data. Retrieved from https://www.oregon.gov/highered/research/Pages/student-data-univ.aspx

IACBE Accreditation (n.d.). Retrieved from http://iacbe.org/memberpdf/OregonInstituteofTechnology.pdf

Institutional Research. (2017). Headcount by Major and Student Type. Retrieved from https://oregontechsfcdn.azureedge.net/oregontech/docs/default-source/institutional-research-documents/major-reports/majors_fall_2017.pdf?sfvrsn=1bd6167_4

Institutional Research. (2017). Quick Facts. Retrieved from https://oregontechsfcdn.azureedge.net/oregontech/docs/default-source/institutional-research-documents/quick_facts_current.pdf?sfvrsn=b3a9c60_4

List of Designated Institutions (2018). Retrieved from:

https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

National Centers for Academic Excellence Case (n.d.) Retrieved from:https://niccs.us-cert.gov/education/national-centers-academic-excellence-cae

Fastest Growing (n.d.). Retrieved from: https://www.bls.gov/ooh/fastest-growing.htm

Roach, R. (2009). The community college transfer problem. Diverse Issues in Higher Education, 26(7), 14-15.