New Certificate Program Proposal
Undergraduate Certificate in CyberSecurity

Status: Pending Review - Faculty Senate Exec Committee (Previous Version)

Hide All Reviews

1. Review - College Approver - Engineering

Approved by Frank Chaplen Associate Professor / Biol & Ecol Engineering, *December 3, 2018 5:43am*

2. Review - Curriculum Coordinator

Sent Back by Janice Nave-Abele Curriculum Coordinator / University Accreditation, *December 3, 2018 10:26am*

Comments

Janice Nave-Abele (Curriculum Coordinator) December 3, 2018 10:26am
Sent back for Originator to add Liaisons.

-Janice
APA

3. Originator Response

Christopher Scaffidi Associate Professor / Sch Elect Engr/Comp Sci, *December 3, 2018 10:31am*

4. Review - Curriculum Coordinator

Sent Back by Janice Nave-Abele Curriculum Coordinator / University Accreditation, *December 3, 2018 4:01pm*

Comments

Janice Nave-Abele (Curriculum Coordinator) December 3, 2018 4:01pm
Proposal is being sent back to the Originator for updates to the wording in the Curriculum section of the proposal.

The elective courses that you indicated as available every term on campus and online are: CS 434, CS 464, CS 475, CS 492, CS 493, and CS 496. Perhaps you meant to use the future tense and indicate that they will be offered every term on campus and online. Currently, it appears that none have been offered every term and CS 434 and CS 492 were not offered at all this past year online. CS 434 and CS 492 will need to be added for the online modality if they haven't been already. BA 480 looks like it also may not have the online modality added. You can check with Rene Reitsma in the CoB on that.

To add the online modality for existing on-campus courses, you do not need to submit a proposal into the CPS. Rather, email Zach Kronser and request that the impacted courses have Ecampus added as a modality. Any brand-new courses will still need to go through the CPS.

In relation to the required courses:

CS 370 – remove the wording about a Cat II proposal in the CPS as all you need to do is email Zach Kronser.

CS 373 - you may remove the wording regarding a Cat II proposal in the CPS as the course has an online modality.

CS 427 - remove the wording about a Cat II proposal in the CPS as all you need to do is email Zach Kron

CS 477 – new course. Please include proposal number – 105438. The proposal must be submitted (not in draft format). The proposal is currently in draft format.

CS 478 - remove the wording about a Cat II proposal in the CPS as all you need to do is email Zach Kronser.

BA 482 – new course in the CPS. Please add the proposal number – 105339. It needs to be submitted as it is still in draft format. Prem Mathew is the Originator on this proposal.

Janice
-APA

5. Originator Response

Christopher Scaffidi Associate Professor / Sch Elect Engr/Comp Sci, *December 19, 2018 8:44am*

Comments

Christopher Scaffidi December 19, 2018 8:44am
Thank you for the feedback.

Because the previous version of the proposal was too coarse-grained in describing the curriculum's modalities and frequencies, the new version explicitly calls out specific proposed modalities and corresponding frequencies for every single course individually. The new version also omits mention of CAT II proposals for the existing courses, as requested. In addition, URLs/numbers have been added for the CAT II proposals of the new courses. The CS 477 CAT II is now submitted out of draft mode, and the originator of the BA 482 CAT II (Prem Mathews) assures me that he will quickly submit that proposal soon.

6. Review - Curriculum Coordinator

Approved by Janice Nave-Abele Curriculum Coordinator / University Accreditation, *December 19, 2018 10:45am*

Comments

Janice Nave-Abele (Curriculum Coordinator) December 19, 2018 10:45am
This NEW Certificate proposal is ready for review by the Budgets and Fiscal Planning Committee and the Curriculum Council.

Luke McIlveney in the BEBC has reviewed the attached four year budgets.

The attached M.O.U. evidences Ecampus support for this proposal.

-Janice
APA

7. Review - Graduate School

Approved by Janice Nave-Abele Curriculum Coordinator / University Accreditation, *December 19, 2018 10:46am*

Comments

Janice Nave-Abele (Graduate School) December 19, 2018 10:46am
The proposal is for a NEW undergraduate Certificate and does not require review by the Graduate School.

8. Review - Budgets and Fiscal Planning Committee

Approved by Andrew Ibarra Dir-Physical Activity Program / Sch of Bio/Pop Hlth Sci, *January 11, 2019 8:47am*

9. Review - Graduate Council Chair

Approved by Lisa Ganio Department Head / Statistics (Science), *January 14, 2019 1:29pm*

Comments

Lisa Ganio (Graduate Council Chair) January 14, 2019 1:29pm
Passing through, this is not a graduate certificate

10. Review - Curriculum Council Chair

Approved by Allen Thompson Associate Professor / Philosophy Department, *January 29, 2019 9:28am*

Comments

Allen Thompson (Curriculum Council Chair) January 29, 2019 9:28am
Proposal was amended at request of CC to require that students take at least one BA course (a non-CS course) in satisfying the electives.

11. Review - Faculty Senate Exec Committee

Sent Back by Janice Nave-Abele Curriculum Coordinator / University Accreditation, *February 19, 2019 9:52am*

Comments

Janice Nave-Abele (Faculty Senate Exec Committee) February 19, 2019 9:52am
Proposal sent back to Originator to upload the most recent version of the Proposal with updates made per the FSEC request. Originator to resubmit after he has uploaded the revised proposal. The proposal will then return to the Faculty Senate Executive Committee's CPS queue.

Janice
-APA

12. Originator Response

Christopher Scaffidi Associate Professor / Sch Elect Engr/Comp Sci, *February 19, 2019 9:56am*

13. Review - Faculty Senate Exec Committee

Pending Review

More Queued Reviews (4)

Faculty Senate; Provost /Academic Affairs; Academic Programs; Catalog Coordinator

Proposal

Proposal ID:105390
Type:New Certificate Program
Submission Date:February 19, 2019 9:56am
Comments:
Program to be delivered on OSU Main - Corvallis, Ecampus, and Portland Satellite (hybrid).

History

Active Version - Submitted February 19, 2019 9:56am
Version 3 - Submitted December 19, 2018 8:44am
Version 2 - Submitted December 3, 2018 10:31am
Version 1 - Submitted November 9, 2018 10:12am

Originators

NAME	TITLE	DEPARTMENT/SCHOOL
Christopher Scaffidi	Associate Professor	Sch Elect Engr/Comp Sci

Contacts

NAME	TITLE	DEPARTMENT/SCHOOL
Carlos Jensen	Assoc Dean-Undergrad Prog	College of Engineering

Proposal Details

College:College of Engineering
Department/School:School of Electrical Engineering and Computer Science
New Certificate Name:Undergraduate Certificate in CyberSecurity

Supporting Documents

DOCUMENTS
* **Signed Transmittal Sheet**
proposal transmittal sheet.pdf (479.69 Kb added Feb 19, 2019 9:52 am)
* **Executive Summary**
Executive Summary.pdf (63.45 Kb added Feb 19, 2019 9:52 am)
* **Proposal**
Cyber CAT1 (revised per new COB course mix).pdf (177.69 Kb added Feb 19, 2019 9:56 am)
* **Letters of Support**
Technology Association of Oregon Letter of support from TAO.pdf (141.46 Kb added Feb 19, 2019 9:52 am)
Hewlett Packard Letter of support from HP.pdf (402.57 Kb added Feb 19, 2019 9:52 am)
* **Accessibility Form**
school commitment to accessibility.pdf (903.59 Kb added Feb 19, 2019 9:52 am)
* **Library Evaluation**
library approval.pdf (81.37 Kb added Feb 19, 2019 9:52 am)
* **Faculty CVs**
Faculty CVs are available upon request.docx (11.06 Kb added Feb 19, 2019 9:52 am)
Other Attachments
Undergraduate Learning Outcomes Assessment.pdf (338.46 Kb added Feb 19, 2019 9:52 am)
20181101 Budget narrative.pdf (54.05 Kb added Feb 19, 2019 9:52 am)
20181101 Budget approved.pdf (116.58 Kb added Feb 19, 2019 9:52 am)

approval by space + facilities.pdf (143.38 Kb added Feb 19, 2019 9:52 am)

Finalized Ecampus MOU.pdf (813.96 Kb added Feb 19, 2019 9:52 am)

LIAISONS

*** Liaisons**

Reindert Reitsma
Request: Version sent to COB Liaison.pdf (764.51 Kb added Feb 19, 2019 9:52 am)
Response: COB Liaison Review.pdf (213.05 Kb added Feb 19, 2019 9:52 am)
CAT I authors' response: Incorporated grammatical edits and narrowed list of Business electives as requested by liaison

Frank Chaplen
Request: CyberSecurity Proposal v20181105 (approved by school).pdf (176.96 Kb added Feb 19, 2019 9:52 am)
Response: Frank Chaplen liaison feedback.pdf (98.32 Kb added Feb 19, 2019 9:52 am)
This liaison chairs the College of Engineering curriculum committee.

Alfonso Bradoch
Request: *None*
Response: *None*
Attached M.O.U. evidences Ecampus support for this proposal.

Erica Curry
Request: *None*
Response: *None*
Attached M.O.U. evidences Ecampus support for this proposal.

Shannon Riggs
Request: *None*
Response: *None*
Attached M.O.U. evidences Ecampus support for this proposal.

BUDGET INFORMATION

*** Budget Year 1**

20181101 Budget.xlsx (23.58 Kb added Feb 19, 2019 9:52 am)
Luke McIveney in the BEBC approved the four year budgets.

*** Budget Year 2**

20181101 Budget.xlsx (23.58 Kb added Feb 19, 2019 9:52 am)
Luke McIveney in the BEBC approved the four year budgets.

*** Budget Year 3**

20181101 Budget.xlsx (23.58 Kb added Feb 19, 2019 9:52 am)
Luke McIveney in the BEBC approved the four year budgets.

*** Budget Year 4**

20181101 Budget.xlsx (23.58 Kb added Feb 19, 2019 9:52 am)
Luke McIveney in the BEBC approved the four year budgets.

Proposal Transmittal Sheet

Full Category I and Abbreviated Category I Proposals

Submit proposals to: Office of Academic Programs, Assessment, and Accreditation
314 Waldo Hall – Oregon State University

Attach Transmittal Sheet; Proposal; Library Evaluation (performed by the Library for Full Category I proposals), Letters of Support (external to OSU); Liaison Correspondence (internal to OSU), External Review (new graduate program proposals), and Budget Information (both OSU and HECC budget sheets for Full Category I proposals and OSU budget sheets for Abbreviated Category I proposals)

Full Category I Proposals: New Programs

Final Approval--for new degrees, extension to OSU's branch campus, and substantive changes:
Higher Education Coordinating Commission (HECC)

Final Approval-- for new certificate programs: OSU Provost

Check one:

- [ ] **New Degree Program**
- [x] **New Certificate Program**
- [ ] **Extend Program to OSU Branch Campus**
- [ ] **Substantive Change**

Abbreviated Category I Proposals: Other Proposals

Final Approval--for new academic units, renames, reorganizations, and, suspensions: OSU Provost

Final Approval-- for terminations: OSU Board of Trustees

Check one:

- [ ] **Establish:** new college, school, department or program
- [ ] **Rename:** change the name of an existing academic program or academic unit
- [ ] **Reorganization:** move the responsibility of an academic program from one academic unit to another; reorganize existing academic unit(s), including mergers and splits
- [ ] **Suspension (or Reactivation):** suspend an academic program (maximum period: three years)
- [ ] **Termination:** terminate an academic program or academic unit

Title of Proposal: Undergraduate Certificate in CyberSecurity

Proposed Effective Term: Summer 2019

School/Department/Program: School of Electrical Engineering and Computer Science

College: College of Engineering

I certify that the above proposal has been reviewed by the appropriate Program, Department, School, and College administrators and committees. I approve this proposal.

	11/5/2018	Thomas Weller, School Head
Sign (Department/School Chair/Head; Director)	***Date***	**Print (Chair/Head; Director)**
	11/6/18	Scott Ashford, Dean
***Sign* (College Dean)**	***Date***	**Print (College Dean)**

Source: Office of Academic Programs, Assessment and Accreditation (2-10-15; rev 1-8-16)

Proposal for the Initiation of an Undergraduate Certificate in CyberSecurity

A single security breach can expose the passwords[1], financial data[2] and private personal information[3] of hundreds of millions of people. The United States government has repeatedly drawn attention to the urgent need for training more cybersecurity professionals to work in both the public and private sectors.[4] Unfortunately, the worldwide shortage of cybersecurity professionals stands at 2.9 million at present,[5] and, if current trends continue, is projected to grow to 3.5 million by 2021.[6]

In response, the College of Engineering proposes an Undergraduate Certificate in CyberSecurity. The proposed program will enable students to understand common threats to system security, assess security requirements for a new or existing system, implement secure solutions to counter threats, and evaluate systems to identify and address weaknesses. It is expected that these skills will enable students to obtain careers in cybersecurity jobs such as cybersecurity analyst, cybersecurity engineer, information assurance technician, and security administrator.

Although, at present, the University only allows students concurrently seeking an undergraduate degree to register for an undergraduate certificate, this policy is currently under revision to permit a new application admissions procedure for qualified students to enroll in certificate programs. Until OSU establishes that new procedure, the proposed undergraduate certificate program will only enroll students concurrently pursuing an undergraduate degree.

The certificate will draw upon existing courses currently offered at the Corvallis campus. These will be adapted for hybrid delivery in Portland and online via Ecampus, thereby enabling students to obtain the certificate through traditional in-person courses in Corvallis, hybrid courses in Portland, online courses via Ecampus, or a mix of the three. The Ecampus funding model will generate sufficient revenue to cover the cost of developing these courses. The School of Electrical Engineering and Computer Science will handle application-processing and advising, and the School's Associate Head for Online and Continuing Education will provide program oversight and review.

---

[1] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[2] https://www.washingtonpost.com/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html
[3] https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html
[4] https://www.gao.gov/products/GAO-18-466
[5] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[6] https://cybersecurityventures.com/jobs/

Proposal for a New Academic Certificate Program

Proposal for the Initiation of a New Instructional Program Leading to an Undergraduate Certificate in CyberSecurity
Oregon State University
College of Engineering
School of Electrical Engineering and Computer Science
CPS Proposal #105390
https://secure.oregonstate.edu/ap/cps/proposals/view/105390

February 2019

1. Program Description

a. Proposed Classification of Instructional Programs (CIP) number

CIP Number: 11.1003
Title: Computer and Information Systems Security/Information Assurance.

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, programming, and systems analysis; networking; telecommunications; 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.

As computer systems have become part of the fabric of modern society, system security has grown essential to the well-being of individuals, companies, the economy and life as we know it. A single security breach can expose the passwords,[1] financial data[2] and private personal information[3] of hundreds of millions of people. According to the Lloyd's insurance company, hacking costs businesses an estimated annual total of $400 billion worldwide, "including the damage itself and subsequent disruption to the normal course of business."[4] Worse yet, flaws in America's power-grid control systems[5] and military systems[6] now put national security at risk. In response, the National Institute of Standards and Technology,[7] the US Government Accountability Office,[8] and the White House under Presidents Trump[9] and Obama[10] have all called for a greater emphasis on securing systems in government and in the private

[1] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[2] https://www.washingtonpost.com/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html
[3] https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html
[4] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/
[5] https://nypost.com/2018/07/23/russian-hackers-could-have-caused-massive-power-outages
[6] https://www.theregister.co.uk/2018/10/15/us_military_weapn_system_vulnerabilities
[7] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[8] https://www.gao.gov/products/GAO-18-466
[9] https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/
[10] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf

sector. Unfortunately, the worldwide shortage of cybersecurity professionals stands at 2.9 million at present[11] and, if current trends continue, will grow to 3.5 million by 2021.[12] The shortage of qualified workers has increased the cost of hiring cybersecurity professionals, who earned an average salary of $116k in 2017.[13] Training the next generation of professionals in cybersecurity has thus become a civic duty for America's higher education system, as well as an economic opportunity for students interested in pursuing careers in cybersecurity-related technology.

In response, the College of Engineering proposes to establish a new Undergraduate Certificate in Cybersecurity. The proposed program will enable students to understand common threats to system security, assess security requirements for a new or existing system, implement secure solutions to counter threats, and evaluate systems to identify and address weaknesses. It expected that these skills will enable students to obtain careers as cybersecurity professionals with job titles that include cybersecurity analyst, cybersecurity engineer, information assurance technician, and security administrator. In addition, these skills will enable students to perform other jobs, such as software engineer and requirements analyst, with a higher level of proficiency and a lower risk of creating security flaws that threaten their users, their employers, their livelihoods, and their nation.

[11] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[12] https://cybersecurityventures.com/jobs/
[13] https://www.cio.com/article/2383451/

Category	Information Summary
Proposal Title	Undergraduate Certificate in CyberSecurity
Proposal Purpose	New Undergraduate Certificate
Classification of Instructional Program (CIP) #	11.1003
Curriculum Proposal System # (incl link)	https://secure.oregonstate.edu/ap/cps/proposals/view/105390
Banner Student Information System (SIS) #	To be assigned by the Registrar's Office
Degree Type (e.g., B.S., M.S., or Ph.D.)	Not Applicable
Program Type (e.g., Undergraduate, Graduate, First Professional)	Undergraduate
Academic Home	College of Engineering
College Code	16
Contacts (e.g,, Name, Title, Tel #, eMail Address)	Dr. Carlos Jensen, Associate Dean 541-737-2555 carlos.jensen@oregonstate.edu
Faculty (New)	No new faculty required for certificate launch
Staff (New)	No new staff required for certificate launch
Library (New)	No new resources required for certificate launch
Facilities/Space (New)	No new buildings, office or labs required for certificate launch
Budget (first four years)	See budget worksheet
Undergraduate Option(s)	Not Applicable

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

Course	Credits	
CS 370	4	Introduction to Security
CS 373	4	Defense Against the Dark Arts
CS 427	4	Cryptography
CS 477	4	Introduction to Digital Forensics
CS 478	4	Network Security
BA 482	4	Information Security Governance
Electives	3	BA 480, CS 434, CS 464, CS 475, CS 492, CS 493, CS 496
TOTAL	**27**	

Most courses listed above already exist for the in-person modality (at the Corvallis campus). The key exceptions are CS 477 and BA 482, which will be new courses (for which CAT II's are already approved).

To satisfy the 3 elective credit hours of the proposed undergraduate certificate program, students will have one choice in business (BA 480) and many choices in computer science. All of these computer science courses are already offered in the Corvallis campus, and most will be available via Ecampus (as described in detail in sub-section d below). These CS courses are:

- CS 434 - Machine Learning and Data Mining (4 credits)
- CS 464 - Open Source Software (4 credits)
- CS 475 - Intro to Parallel Programming (4 credits)
- CS 492 - Mobile Software Development (4 credits)
- CS 493 - Cloud Application Development (4 credits)
- CS 496 - Mobile/Cloud Development (4 credits) [will be phased out, replaced with 492/493]

Such courses provide venues for applying concepts from cybersecurity. For example, the Open Source Software course (CS 464) includes a learning outcome that involves contributing to an existing open source project, which for a student interested in cybersecurity could involve contributing a security fix to an existing project.

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).

Courses for the proposed certificate program will be offered at the frequencies, modalities and locations shown below.

Course	In-person in Corvallis	Hybrid via Ecampus + Portland (Meier & Frank Building)	Online via Ecampus
CS 370	Once per year	At least once per year	At least once per year
CS 373	Once per year	At least once per year	At least once per year
CS 427	Once per year	At least once per year	At least once per year
CS 477	Once per year	At least once per year	At least once per year
CS 478	Once per year	At least once per year	At least once per year
BA 482			At least once per year
CS Electives	434, 464 and 475: each at least once per year 492, 493, 496: every year, at least 2 of these 3 will be offered at least once		464 and 475: each at least once per year 492, 493, 496: every year, at least 2 of these 3 will be offered at least once
BA Elective	480: once per year		

The unusual frequency of the 492/493/496 combination in the table above is due to the fact that EECS is currently phasing 496 out by splitting it into two courses, 492 and 493. After 496 is gone, 492 and 493 are each anticipated to be offered at least once per year.

Given sufficient demand, the frequency of hybrid and Ecampus offerings might increase. Hybrid offerings for the 5 required courses might increase to every other term, and the hybrid modality could possibly be added in the future for the CS electives. Ecampus offerings for courses currently available online might increase to every term. Increasing any course's frequency beyond a rate shown in the table above will depend not only on the number of students enrolled in the proposed undergraduate certificate program itself (section f, below), but also on the number of other students who want to take the course.

e. Ways in which the program will seek to assure quality, access, and diversity.

Even though it is anticipated at present that almost all students enrolling in the proposed certificate program will be enrolled in the Bachelor's or Post-Baccalaureate degree programs in *computer science*, other students are anticipated to be enrolled in a *business-related* undergraduate program. Longer-term, it is possible that students pursuing undergraduate degrees in *other* fields might also wish to obtain a certificate in cybersecurity. The reason is that cybersecurity is becoming an important issue in civil

engineering,[14] smart manufacturing,[15] farming,[16] political science,[17] and a broad range of other fields. All undergraduate students will be welcome to pursue the proposed cybersecurity certificate, provided that they are adequately qualified (as defined below).

Although, at present, OSU only allows students concurrently seeking an undergraduate degree to register for an undergraduate certificate, this policy is currently under revision at the university level to permit a new application admissions procedure for qualified students to enroll in certificate programs. Until OSU establishes that new procedure, the proposed certificate program will only enroll students concurrently pursuing an undergraduate degree. Once OSU has established a procedure for students to enroll directly in undergraduate certificate programs, then qualified students will also be able to enroll in the proposed cybersecurity undergraduate certificate program.

Student qualifications: The School of Electrical Engineering and Computer Science will review all applications to ensure that applicants are concurrently pursuing an undergraduate degree at Oregon State University, have a GPA of at least 3.0, and have obtained at least a C in the prerequisite courses of the required degree program courses (i.e., CS 261 Data Structures, CS 340 Introduction to Databases, CS 344 Operating Systems, and CS 372 Computer Networking). As noted above, the University anticipates eventually allowing students to enroll directly into undergraduate certificate programs (i.e., without concurrently seeking an undergraduate degree); such students will still need to meet the GPA and the prerequisite requirements, above (in addition any university-level requirements on such students).

Access: In order to increase the availability of the proposed certificate program to students who might take a non-traditional track through their education, applicants with 3+ years of professional experience as software or system engineers will be allowed to petition for the waiver of one or more prerequisites. Decisions regarding waivers will be at the discretion of instructors.

Student success: The School's academic advisors[18] will be available on-demand to guide potential students regarding appropriateness of the proposed certificate program for their career goals, to help students select career-relevant electives, and to coach struggling students. A team of 4-5 Ecampus advisers and coaches[19] guide students on following policies, obtaining exam proctors, setting goals, managing time, and similar student-success topics.

Diversity: The College of Engineering, in coordination with the College of Business, designed the electives component of the curriculum with the intention of accommodating the diverse interests of students, with a particular focus on students who may be pursuing a major in business or another field (e.g., with the intention of ultimately pursuing a career in management at a technology company). The proposed program will accommodate students from diverse backgrounds, including those residing in Portland's urban setting, by delivering the curriculum via a range of modalities and locations. Furthermore, it is anticipated that the availability of evening courses in the Portland satellite facility location will aid in accommodating the needs of students who cannot afford to stop working while going to school and who therefore must schedule courses around job-related constraints.

[14] https://www.afcec.af.mil/News/Article-Display/Article/1319284/
[15] https://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/
[16] https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data
[17] https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/
[18] http://eecs.oregonstate.edu/current-students/undergraduate/advising
[19] https://ecampus.oregonstate.edu/services/student-services/

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

Approximately 12-18 students are expected to enroll each year. The number will probably start at the lower end of that range in the first year, then grow toward the upper end by the fifth year.

Academic year	Estimated Headcount	Estimated FTE	Cumulative Est. Completions
2019-20	12	6	12
2020-21	14	7	26
2021-22	15	7.5	41
2022-23	16	8	57
2023-24	18	9	75

g. Expected degrees/certificates produced over the next five years.

Each student will typically complete the proposed undergraduate certificate program in one year. If an average of 15 complete the proposed certificate program per year during the first five years, as expected, then a total of 75 will complete the proposed certificate program by the end of that period (see table above).

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

The program will primarily serve students concurrently pursuing an undergraduate degree (as noted above in section e). Most of the students are expected to be traditional, resident, full-time students pursuing a Bachelor's degree in computer science at the Corvallis campus. A smaller group of students will be non-traditional students pursuing the Post-Baccalaureate Bachelor's degree in computer science (generally part-time via Ecampus), some of whom will live in the Portland area; others will be non-residents. A still smaller group of students are expected to be traditional, resident, full-time students pursuing a Bachelor's degree in a business field with a minor or an interest in computer science. It is expected that in the longer-term, some students from other fields might wish to enroll in the proposed certificate program (as noted in section e), though this is speculative at present. Eventually, once OSU has established a procedure for enrolling directly into undergraduate certificates without a concurrent degree program, the proposed cybersecurity certificate program is expected to serve software engineers in the Portland area (as part-time students via Ecampus and/or hybrid courses at the Portland satellite).

i. Adequacy and quality of faculty delivering the program.

The team leading, developing and delivering the first year of the program includes the following:

- Chris Scaffidi: PhD in Software Engineering; Associate School Head in OSU's School of Electrical Engineering and Computer Science; Associate Professor; has created 3 of the core 15 courses in the Computer Science Post-Bacc program; has taught and researched software engineering and other computer science topics at OSU for 9 years; has served as school liaison to the Technology Association of Oregon; has worked previously for 6 years as a professional software engineer.
- Rakesh Bobba: PhD in Electrical and Computer Engineering; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched security and other

computer science topics at OSU and the University of Illinois for 9 years; has served as Co-PI for multiple federally-funded cybersecurity projects; serves on the Oregon Cybersecurity Advisory Council, established in 2017 to advise the State Chief Information Officer on cybersecurity matters and to develop a shared vision for the establishment of a cross-sector Cybersecurity Center of Excellence.

- Mike Rosulek: PhD in Computer Science; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched cryptography and other computer science topics at OSU and the University of Montana for 9 years; has an internationally-recognized reputation as a cryptographer; has helped to lead the International Association for Cryptologic Research.
- Dave Nevin: MA in English; Director of the Oregon Research & Teaching Security Operations Center and adjunct to the School of Electrical Engineering and Computer Science; has 20+ years in systems security, architecture and administration; Certified Information Systems Security Professional; experience developing and implementing security policies; experience with training information technology staff in security practices; familiar with numerous laws, standards, policies and regulations bearing on security including EU-GDPR, FERPA, CUI/ NIST SP800-171, PCI-DSS, and Export Control.
- Jesse Walker: PhD in Mathematics; Research Professor and adjunct to the School of Electrical Engineering and Computer Science; previously was Intel's Chief Cryptographer; has collaborated on research and development of security-related aspects of system design for approximately two decades; achieved international impact for discovering a key weakness in what was the most widely-used wireless protocol (WEP), as well as for helping to invent replacement protocols (WPA and WPA2) now in widespread use.
- Kevin McGrath: MS in Computer Science; Senior Instructor in the School of Electrical Engineering and Computer Science; also Security Researcher at McAfee Advanced Threat Research Lab; has taught and researched operating system design and security, as well as other computer science topics, at OSU for 7 years.

j. Faculty resources – full-time, part-time, adjunct.

The first three faculty above are full-time (but will work part-time on leading the proposed certificate program), while the others are part-time.

k. Other staff.

The proposed undergraduate certificate program will be supported by existing staff in the School of Electrical Engineering and Computer Science and in Ecampus. These include:

- The Associate School Head for Online Programs (Section 1.i) will inform and oversee creation of courses for the hybrid and online modalities, as well as lead the evaluation of the program and its teachers.
- The Admissions Coordinator will review student applications per the criteria above (Section 1.e)
- Academic Advisers, including 3-4 in the School plus 4 in Ecampus, together will serve the existing student population both on-campus and online to promote student success (Section 1.e).
- At least one 0.49 FTE graduate Teaching Assistant per course, and/or additional "pool" TAs dedicated to serving Ecampus and hybrid students across all courses in the Portland area, will hold weekend office hours downtown.

l. Facilities, library, and other resources.

The current facilities, library and other resources will adequately support the proposed certificate program.

m. Anticipated start date.

Summer Term 2019 (Banner: 202000)

2. Relationship to Mission and Goals

a. Manner in which the proposed program supports the institution's mission and goals for access; student learning; research, and/or scholarly work; and service.

Security flaws can harm individual consumers worldwide, as well as Oregon companies and others that sell or service affected software. Mistakes that affect military systems, electricity infrastructure, and other mission-critical systems can even threaten the national security of the United States. Therefore, offering a new undergraduate certificate program in the high-impact area of cybersecurity will align with the University's commitment to promote the well-being of Oregon, the nation, and the world. Moreover, the proposed certificate will support the University's education mission by preparing students for obtaining jobs in cybersecurity-related careers.

b. Connection of the proposed program to the institution's strategic priorities and signature areas of focus.

Establishing a technically proficient workforce is essential to Oregon's economic development, and it ties directly to the Healthy Economy strategic priority of OSU.

c. Manner in which the proposed program contributes to Oregon University System goals for access; quality learning; knowledge creation and innovation; and economic and cultural support of Oregon and its communities.

Section 1.e discusses in detail how different aspects of the proposed program will contribute to quality learning, access, and diversity. Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

d. Manner in which the program meets broad statewide needs and enhances the state's capacity to respond effectively to social, economic, and environmental challenges and opportunities.

Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

3. Accreditation

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

There is no internationally-adopted standard for cybersecurity education, although several companies and societies offer certifications of their own for different subsets of cybersecurity. The closest standard that spans all potential students' interest areas is from NIST's National Initiative for Cybersecurity Education (NICE). Specifically, the NICE Cybersecurity Workforce Framework[20] characterizes the ways in which

[20] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

different cybersecurity professions are similar or different in terms of the capabilities required of professionals.

This framework was used, in combination with a review of the diverse career directions that students are anticipated to take, to identify core technical knowledge and skills essential to a range of different career paths. These core capabilities were then incorporated as learning outcomes into required courses of the proposed certificate program. Finally, the proposed certificate program was designed to require students to pursue additional elective credits in an area relevant to their respective long-term career interests.

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.

Not applicable

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.

Not applicable, as there is no applicable accreditation standard.

4. Need

a. Evidence of market demand.

As described in Section 1.a, millions of high-paying jobs in cybersecurity are going unfilled. Relevant statistics include:

- 2.9 million unfilled positions estimated in 2018[21]
- 3.5 million unfilled positions projected in 2021[22]
- Growth rate forecast at 37% from 2012-2022[23]
- Average salary $116k in 2017[24]
- Entry level salary $66k in 2018[25]
- Steep payscale, rising to $233k for chief information security officers in 2018[26]

The underlying source of market demand for cybersecurity professionals is the burgeoning number of massive, expensive security flaws. Relevant statistics include:

[21] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[22] https://cybersecurityventures.com/jobs/
[23] https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs
[24] https://www.cio.com/article/2383451/
[25] https://tinyurl.com/payscale-entry-level-cyber-sec
[26] https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000

- 5,000 publicly revealed breaches in 2017[27]
- 189,445 total known security vulnerabilities in commercial software since 2011, including 17,091 in 2018[28]
- Over 19 billion records affected in total from known breaches between 2015-2018[29]
- Average cost of $7.3M per security breach in the United States in 2017[30]
- $4.7B projected revenue for digital forensics firms (alone) in 2020[31]

As long as the pace and impact of security breaches continues to accelerate, market demand for cybersecurity professionals will likely remain strong, as well.

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

Not applicable

c. Manner in which the program would serve the need for improved educational attainment in the region and state.

It is anticipated that the proposed certificate program will help students to advance in their current job or to obtain a more preferred position where they can use their new skills.

d. Manner in which the program would address the civic and cultural demands of citizenship.

As noted in Section 1.a, security flaws threaten the well-being of companies, individuals, and the nation. Many student learning outcomes of required courses within the proposed certificate program therefore pertain to civic and cultural life. To illustrate, consider the first two of these required courses:

- CS 370 - Introduction to Security: This course teaches students about typical threats to privacy, security, accountability and similar fundamental attributes demanded of the systems that pervade everyday life. The course thereby enables students to achieve the learning outcome to "Understand the need for cyber security, key notions of security, and well established security principles and security mechanisms/controls."
- CS 373 - Defense against the Dark Arts: This course teaches students in further detail about threats to security in modern society, so that they can "Demonstrate awareness of the current state of malware, adware, and crypto-ware." Furthermore, it teaches techniques to counter these threats. For example, two other learning outcomes are that students can "Implement spam identification tools" and can "Implement solutions to common attack vectors in multiple environments." The course thus teaches students how to protect against the malware that frequently takes over peoples' computers, against the spam that chokes their communications, and against the crypto-ware that encrypts the hard drives of consumers and companies (then demands a ransom).

[27] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[28] https://vulndb.cyberriskanalytics.com/
[29] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[30] https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html
[31] https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html

5. Outcomes and Quality Assessment

a. Expected learning outcomes of the program.

Students completing the proposed certificate program will be able to:

- Describe the common threats to system security and explain their mechanisms of action
- Assess system requirements pertaining to confidentiality, integrity, and availability of data and functionality to users
- Implement secure solutions to common threats by selecting and applying appropriate principles, protocols and techniques
- Evaluate system designs, implementations and protocols to identify and ameliorate weaknesses

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

Every other spring, the Associate School Head for Online and Continuing Education will email students enrolled in the undergraduate certificate program, inviting them to complete a questionnaire about their perception of what they have learned related to the program learning outcomes. This questionnaire will be designed with the input of the courses' instructors so that, for each of the 4 program learning outcomes, the questionnaire specifies specific elements of specific courses with related course-level learning outcomes. The questionnaire will ask students to rate the effectiveness of those course elements in helping students to achieve the corresponding program-level learning outcomes.

Then, learning outcomes will be identified for which relatively few course elements were rated relevant or beneficial. The Associate School Head will then conduct focus groups with the instructors to solicit their perceptions about the strengths and weaknesses of courses relative to learning outcomes, as a means of cross-validating students' perceptions about these course elements. These conversations with instructors will also aim to identify strategies for improving the curriculum during the subsequent year. Finally, in the following year, the next round of questionnaires will make it possible to assess the extent to which these changes improved student learning outcomes.

c. Program performance indicators, including prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate.

The College of Engineering performs a yearly survey of recent BS graduates using a questionnaire similar to that of the National Association of Colleges and Employers (NACE) First-Destination Survey. The College will augment this survey with new questions enabling it to measure the percent of certificate graduates who report obtaining a job that involves designing, implementing, troubleshooting or managing security-related aspects of systems. These questions will already be part of the survey deployed prior to the graduation of the first cohort of students in the proposed certificate program, thereby providing a baseline for comparison when assessing whether the program aids students in obtaining measurably better career outcomes. In addition, these questions will be part of the survey given to all computer science graduates in the future, making it possible to assess whether students graduating with the proposed undergraduate certificate achieve better career outcomes on the target metric than students lacking the certificate.

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

The College of Engineering has established expectations for the nature and level of research and/or scholarly activity of faculty. The School of Electrical Engineering and Computer Science evaluates all tenure/tenure-track faculty on an annual basis to ensure they meet expectations, and the College of Engineering reviews all faculty considered for tenure and promotion. The proposed undergraduate certificate program will not impact any of these expectations for research and/or scholarly work.

6. Program Integration and Collaboration

a. Closely related programs in other OUS universities and Oregon private institutions.

Several Oregon institutions offer somewhat topically-related initiatives.

- Oregon Institute of Technology (OIT) operates a Cyber Defense Center, within which students learning cybersecurity can practice on companies facing security issues. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[32]
- Portland State University (PSU) has hosted GenCyber summer camps for high schoolers. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[33]
- Mt. Hood Community College (MHCC) offers an Associate of Applied Science in Information Systems and Technology Management in Cyber Security and Networking. The program focuses on hardware- and networking-related aspects of security. It is therefore narrower than the proposed certificate program, which will address hardware, network, software, protocol, mathematical and management aspects of system security.[34]

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.

After the proposed undergraduate certificate program has been implemented, collaborating with the programs above could provide avenues for expanding student headcount and program impact. For example, PSU actively recruits other organizations (including universities) to host their summer camps; serving as a PSU GenCyber camp could enable OSU to more effectively reach seniors in high school, as a means of exciting them about applying to OSU to study cybersecurity further.

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

See 6.b above. Creating a cybersecurity certificate will establish credibility as a potential partner to other organizations and open up opportunities for collaboration.

d. Potential impacts on other programs in the areas of budget, enrollment, faculty workload, and facilities use.

None anticipated.

---

[32] https://www.oit.edu/cyber-defense-center
[33] https://www.gen-cyber.com/
[34] https://www.mhcc.edu/CyberSecurityNetworkingCurriculum/

7. Financial Sustainability (attach Budget Outline)

a. Business plan for the program that anticipates and provides for its long-term 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.

Existing School staff supporting ongoing programs will suffice for offering the proposed certificate program. The curriculum will adapt existing courses, and the College has budgeted for this one-time expense. Faculty teaching the proposed undergraduate certificate program through the first year have already been identified. In addition, a standing hiring committee has been established to continually accept and evaluate applications for positions as instructors across all teaching modalities and locations (Corvallis in-person courses, Ecampus fully-online courses, and Portland hybrid courses). No new demands on library resources are anticipated.

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

None anticipated.

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

To obtain their required 27 credit-hours for the proposed certificate program, students will typically take 7 courses, which approximately equals the number of sections taught by a 1.0 FTE instructor. Because the projected certificate enrollment is expected to be approximately 15 students (7.5 FTE) per year, the College of Engineering therefore targets a 7.5 student:faculty FTE ratio. The impact on class size is not anticipated to be significant, as the College plans to split sections so they rarely grow beyond 50 students each. This cap is consistent with studies indicating such sizes help contain costs relative to smaller courses,[35] with little negative impact on student outcomes relative to smaller courses.[36,37] In fact, one study indicated that students reported having more meaningful peer interaction in sections of 20-40 students than students did in smaller sections.[38]

d. Resources to be devoted to student recruitment.

The College of Engineering has budgeted for a marketing campaign to be conducted in partnership with Ecampus, as a means of highlighting the College's Portland presence and the availability of the proposed undergraduate certificate program.

---

[35] Bettinger, E., Doss, C., Loeb, S., Rogers, A., & Taylor, E. (2017). The Effects of Class Size in Online College Courses: Experimental Evidence. *Economics of Education Review*.

[36] Gorman, C., Webb, D., & Gee, K. (2018). Hierarchical Linear Modeling Approach to Measuring the Effects of Class Size and Other Classroom Characteristics on Student Learning in an Active-Learning Based Introductory Physics Course. arXiv preprint arXiv:1809.00218. https://arxiv.org/ftp/arxiv/papers/1809/1809.00218.pdf

[37] Monks, J. & Schmidt, R. (2011). The Impact of Class Size on Outcomes in Higher Education. *The B.E. Journal of Economic Analysis & Policy, 11*(1), doi:10.2202/1935-1682.2803.

[38] Burruss, N., Billings, D., Brownrigg, V., Skiba, D., & Connors, H. (2008). Class Size as Related to the Use of Technology, Educational Practices, and Outcomes in Web-Based Nursing Courses. *Journal of Professional Nursing*. DOI: https://doi.org/10.1016/j.profnurs.2008.06.002

8. External Review
(if the proposed program is a graduate level program)

Not applicable

TECHNOLOGY ASSOCIATION OF OREGON

23 October 2018

Carlos Jensen, Ph.D.
Associate Dean
College of Engineering
Oregon State University

Dear Dr. Jensen:

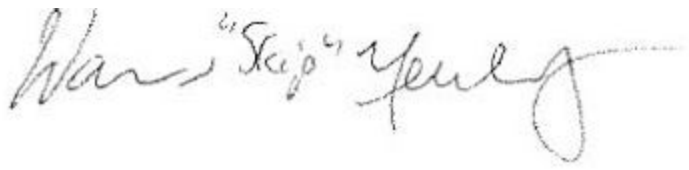
Thank you for the opportunity to express the strong support of the Technology Association of Oregon (TAO) for your college's proposed Undergraduate Certificate in Cyber Security.

TAO's mission is to unite the region's technology industry, and our organization's members include Intel, McAfee, Mozilla, RSA, Tripwire and dozens of other companies who face cybersecurity challenges every day. TAO launched a Cyber Security Committee in 2016 to help our members establish partnerships and build solutions to these security challenges. Since then, our committee's events, including a Cyber Security Summit in 2017, have further revealed that the need for cybersecurity professionals is deeper, more urgent and more pervasive every day.

Consequently, we anticipate that TAO members will eagerly seek graduates of the proposed certificate. In addition, we are especially pleased to see that your college will provide these courses via your Portland facilities and via your highly-respected E-Campus. Delivering your courses via these venues will make it easier for practicing professionals to take classes to advance their skills and their companies' success.

In view of this pressing need for more cybersecurity professionals, it would be hard to overstate TAO's support for the proposed certificate. Furthermore, we will be happy to discuss how to share information about the certificate program with members of TAO. We enthusiastically anticipate the approval of this program and look forward to continued conversations.

Sincerely,



Skip Newberry

President & CEO, Technology Association of Oregon

HP Inc.
1000 NE Circle Blvd
Corvallis, OR 97330

hp.com

October 30, 2018

Carlos Jensen
Associate Dean
College of Engineering
Oregon State University
101 Covell Hall
Corvallis, OR 97331

Dear Carlos,

I am writing to express my support for adding a new Undergraduate Certificate in CyberSecurity at Oregon State University. This certificate aligns well with other interests HP shares with OSU including IoT, Big Data, and AI. HP has made significant investments in cybersecurity. For example, one of our four labs at HP Labs is devoted to cybersecurity. Our Security and Privacy Affinity Group (a self-selected technical community) has over 300 members. These investments, among many others, have contributed to Hewlett-Packard's status as a leader in security. We take pride, for example, in being able to claim we have the world's most secure printers. Our company continues to invest in expanding our status as a leader in security and we strive to hire outstanding engineers and other professionals who have a strong background in cybersecurity. The new certificate program proposed by the College of Engineering will help to prepare the next generation of workers in this vitally important area of expertise. Therefore, we strongly support the creation of this program and eagerly look forward it its swift launch.

Sincerely,

Timothy L. Weber, Ph.D.
Global Head of 3D Metals

ACCESSIBILITY
New Program Proposal (Degree or Certificate)
Guidelines for Addressing Accessibility

Sections 503 and 504 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act of 1990 (ADA), as amended by the ADA Amendments Act of 2008 prohibits discrimination on the basis of disability. The Rehabilitation Act and the ADA require that no qualified person shall, solely by reason of disability, be denied access to, participation in, or the benefits of, any program or activity operated by the University. Each qualified person shall receive the reasonable accommodations needed to ensure equal access to employment, educational opportunities, programs, and activities in the most integrated setting feasible.

For questions and assistance with addressing access, please contact:
the Office of Disability and Access Services (737-4098), or
the Office of Affirmative Action and Equal Opportunity (737-3556).

Title of Proposal: Undergraduate Certificate in CyberSecurity

Date: 5 Nov 2018

School/Department/Program: School of Electrical Engineering & Computer Science

College: College of Engineering

- ☒ Accessibility (http://oregonstate.edu/accessibility/policies)
- ☒ Faculty Guidelines (http://ds.oregonstate.edu/facultyguidelines)
- ☒ Information Technology Guidelines (http://oregonstate.edu/accessibility/ITpolicy)

By signing this form, we affirm that at we have reviewed the listed documents and will apply a good faith effort to ensure accessibility in curricular design, delivery, and supporting information.

Sign (School/Department/Program Director/Chair/Head)

Thomas Weller, School Head

Print (School/Department/Program Director/Chair/Head)

11/5/2018

Date

Source: Office of Academic Programs, Assessment, and Accreditation (glb/ch; 4-26-16)

OSU Libraries & Press (OSULP)
Library Evaluation for Category I Proposal for Proposal for a New Academic Certificate Program

Proposal for the Initiation of a New Hybrid Instructional Program Leading to an Undergraduate Certificate in CyberSecurity

Title of Proposal

School of Electrical Engineering and Computer Science
Department

College of Engineering
College

The Associate University Librarian for Research & Scholarly Communication has assessed whether the existing library collections and services can support the proposal. Based on this review, the present collections and services are:

[ ] inadequate to support the proposal (see budget needs below)
[ ] marginally adequate to support the proposal
[X] adequate to support the proposal

Estimated funding needed to upgrade collections or services to support the proposal (details are attached)

Year 1: Ongoing (annual):

Comments and Recommendations:

It should be noted that Oregon State's Portland campus is a new location, and the workflows for providing access to information (physical and digital) have not been tested. At the current time, we anticipate that the workflows developed for serving Ecampus programs will be adequate, but it is possible that unanticipated needs may arise in the future. Therefore, if a critical resource need arises that current OSULP collections and services cannot meet, The College of Engineering, The School of Electrical Engineering and Computer Science , E-campus and OSULP should work together to solve the resource need.

Date Received: 10/26/18 Date Completed: 11/06/2018

Cheryl A. Middleton
Associate University Librarian for Research & Scholarly Communication

Cheryl A. Middleton
Signature

11/6/2018
Date

Faye A. Chadwell
Donald and Delpha Campbell University Librarian and OSU Press Director

Faye A. Chadwell
Signature

11/6/2018
Date

Oregon State University Libraries Evaluation of the Collection supporting a Proposal for the Initiation of a New Instructional Program Leading to an Undergraduate Certificate in CyberSecurity

This is an expediated library review in support of a new Hybrid Undergraduate Instructional Program Certificate in Cybersecurity. The majority of the courses being proposed for this certificate with the exception on 1 course, CS477 Digital Forensics, are courses that currently exist in the Computer Science program of the School of Electrical Engineering and Computer Science degree program. Those courses are adequately supported by Oregon State University Library and Press Collections.

OSULP Collections

Given that the The Portland Hub does not have a local branch library, students will have access to all electronic resources available through OSULP and will be able to request print materials from the OSULP collections to be sent to their home addresses. The existing agreements that cover the costs of delivering print library materials to Ecampus-only students will apply to students designated as participants in the new instructional program leading to an undergraduate certificate in CyberSecurity.

The growing availability of e-books makes it possible to expedite access to more information from various locations. This obviously better serves our distance learners. As the proposed program will also be located off the Corvallis campus at the Portland Hub and through E-campus, facilitating access is essential. OSULP has a collection of over 800,000 e-books available.

OSU is served well by the OSULP' investment in the Orbis/Cascades Alliance, an Alliance of 39 academic libraries in Oregon, Washington, and Idaho, whose combined collection is substantial. Students and faculty can order from the collections of all the libraries in the Orbis Cascade Alliance through the Summit catalog.

The majority of OSULP subscriptions are for electronic journals, so students can access articles from any location through their official OSU account. Print articles located in the OSULP collections may be requested via the Scan and Deliver service, which provides PDFs of the requested articles. For materials not available in OSULP collections or through Summit, Interlibrary Loan (ILL) is available to borrow items from other libraries.

Instruction Services

Library faculty help students develop information literacy skills--the ability to locate, evaluate, and use information effectively--and help students understand their lifelong roles and responsibilities as both consumers and creators in the information ecosystem. More information on library instruction is available at https://library.oregonstate.edu/instruction-services.

The Library Liaison for the College of Engineering is Lindsey Marlow. Liaisons are library faculty members monitor the strategic directions and priorities of college and programs, and are a conduit to the expertise and services of the OSU Libraries. They promote OSULP expertise and collaborate with Library Experts to integrate and leverage that expertise throughout the OSU Community.

Faculty CVs are available upon request.

CAT I authors' note:

*The reviewer's feedback (**see next page**) was in response to the following draft of Section 5.*

5. Outcomes and Quality Assessment

a. Expected learning outcomes of the program.

Students completing the proposed certificate program will be able to:

- Describe the common threats to system security and explain their mechanisms of action
- Assess the security requirements for a proposed or existing system
- Implement secure solutions to common threats by selecting and applying appropriate principles, protocols and techniques
- Evaluate system designs, implementations and protocols to identify and ameliorate weaknesses

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

Every other spring, the Associate School Head for Online and Continuing Education will email students enrolled in the undergraduate certificate program, inviting them to complete a questionnaire about their perception of what they have learned related to the program learning outcomes. This questionnaire will be designed with the input of the courses' instructors and, for each of the 4 program learning outcomes, will aim at uncovering what elements of specific courses were most and least helpful in achieving that learning outcome. Then, learning outcomes will be identified for which few course elements were relevant or beneficial. The Associate School Head will then collaborate with the instructors to identify and implement strategies for improving the curriculum during the subsequent year. Then, in the following year, the next round of questionnaires will make it possible to assess the extent to which these changes improved student learning outcomes.

c. Program performance indicators, including prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate.

The College of Engineering performs a yearly survey of recent BS graduates using a questionnaire similar to that of the National Association of Colleges and Employers (NACE) First-Destination Survey. The College will augment this survey with new questions enabling it to measure the percent of certificate graduates who report obtaining a job that involves designing, implementing, troubleshooting or managing security-related aspects of systems. These questions will already be part of the survey deployed prior to the graduation of the first cohort of students in the proposed certificate program, thereby providing a baseline for comparison when assessing whether the program aids students in obtaining measurably better career outcomes. In addition, these questions will be part of the survey given to all computer science graduates in the future, making it possible to assess whether students graduating with the proposed undergraduate certificate achieve better career outcomes on the target metric than students lacking the certificate.

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

The College of Engineering has established expectations for the nature and level of research and/or scholarly activity of faculty. The School of Electrical Engineering and Computer Science evaluates all tenure/tenure-track faculty on an annual basis to ensure they meet expectations, and the College of Engineering reviews all faculty considered for tenure and promotion. The proposed undergraduate certificate program will not impact any of these expectations for research and/or scholarly work.

Outcomes and Quality Assessment

1. Observation: Three of the four outcomes are well-written, measurable outcomes that include enough detail to adequately explain student expectations. The second learning outcome, “Assess the security requirements for a proposed or existing system,” does not match the rigorous detail of the other three outcomes.

Recommendation: As currently written, this outcome is still a measurable outcome, but could benefit from expanded language that brings it into alignment with the other learning outcomes.

2. Observation: None of the existing learning outcomes include language that refers to “user” needs or issues. Identifying or analyzing users’ security issues was part of at least one learning outcome in most of the various institutions I researched with a cybersecurity program(within our region and around the nation).

Recommendation: “Identifying and analyzing a user’s security requirements” is language that could be easily integrated into the second listed outcome, “Assess the security requirements for a proposed or existing system.”

3. *Observation:* Program level assessment is completely dependent on a single indirect assessment method, a student questionnaire. This questionnaire is an excellent tool and will provide good feedback to the program, but does not provide enough information to the program or satisfy requirements for direct assessment.

Recommendation (1): Consider expanding the indirect assessment to the instructors as well. Surveys completed by teaching faculty can provide a different insight than student feedback.

Recommendation (2): Direct assessment methods need to be identified for each of the four learning outcomes. This is usually done by finding the courses with matching learning outcomes and identifying assessments within those courses. For instance, CS 373 (mentioned in the proposal) has at least three course outcomes that directly align with program outcomes: “Demonstrate awareness of the current state of malware, adware, and crypto-ware,” “Implement spam identification tools,” and “Implement solutions to common attack vectors in multiple environments.” The exams, projects and other assignments used to measure these course outcomes within CS 373 could also be used for program level assessment.

CAT I authors’ responses to recommendations:

1. Expanded wording of second learning outcome to add detail as recommended
2. Revised second learning outcome to incorporate relationship to user as recommended
3. (1) Revised Section b to include soliciting feedback from instructors, as well (focus groups).
   (2) Revised Section b to explicitly note the survey’s linkage between program-level learning outcomes and the elements of specific courses intended to prepare students in those areas

Budget Narrative

Courses

The proposed undergraduate certificate program will involve 5 required courses and a range of potential electives.

Course	Credits	Title
CS 370	4	Introduction to Security
CS 373	4	Defense Against the Dark Arts
CS 427	4	Cryptography
CS 477	4	Digital Forensics
CS 478	4	Network Security
Electives	7	Various options, some in BA and some in CS; none relevant to this budget document, as EECS will offer them regardless
TOTAL	**27**	

All five of the required courses, above, will be adapted to the hybrid and online modalities. (CS 373 already exists as an online course but will undergo a full updating to the state of the art.)

All of the electives are omitted from the following analyses. They either already exist within COE as on-campus and online courses, or they are already being created and separately budgeted within COE.

One-time budget

One-time costs

COE projects a cost of $75,000 to cover faculty salary (typically spent as overload) associated with creating the 5 hybrid and online modalities of the courses. In addition, COE budgets OPE at 50% of salary for this work.

COE projects a cost of $5,000 for marketing the program, as part of the launch.

One-time resources

COE already has a budget of $110,000 from prior funds for the certificate launch.

COE anticipates receiving $75,000 from Ecampus, at a rate of $15,000 for each of the 5 courses to be re-created for delivery in the online modality.

Recurring budget

Recurring costs

COE projects a cost of $60,000 to cover faculty/instructor salary associated with offering each of the 5 courses once per year.

In addition, another $25,000 is allocated for a coordinator role, expected to help support the program and to get it off the ground during the 1st three years. If enrollment grows at the conservative rate used in the analysis below (to only 18 students in year 5), then by the 4th year, it is expected that the program will be stable and leave no need to maintain an explicit coordinator role. On the other hand, as noted in the Discussion section below, enrollment could grow beyond projections, in which case a coordinator could be added for Year 4 and beyond.

Salaries are projected to increase at 3% annually. OPE is budgeted at 50% of salary.

COE projects marketing expenses of $500 per year after the first year. (See above in One-time costs for first-year marketing expense.)

COE projects $2500 for travel expenses in each of the four years.

Recurring revenues and other resources

Revenue is estimated based on the model currently used by Ecampus courses, which pays COE 80%*($487-$82) = $324 per student credit hour. Each student will take 5*4=20 credits for the required courses involved in this analysis during the 1-year certificate. In addition, COE will obtain revenue from certificate completions, at an estimated $3000 per certificate completion. Conservatively, no future tuition increases are projected.

Discussion

In all years, the revenue is projected to exceed costs. Should revenue in excess of costs materialize, as projected, then the college can invest the additional revenues in several ways. Possibilities include:

- Maintaining the Coordinator position beyond the 3rd year, particularly if enrollment grows faster than anticipated.
- Hiring TAs to support the courses (which, as reflected in the budget here, is typically not the case for undergraduate class sizes of 18 or fewer, but would be appropriate if enrollment proves larger than projected)
- Offering online or hybrid courses more frequently than once per year (perhaps even as frequently as once per term online, as is the case for most online courses in the computer science program)
- Expanding marketing efforts (beyond the indicated budget)
- Hiring additional advisers (proportionate to the number of students enrolled)

Christopher Scaffidi

From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Thursday, November 01, 2018 1:34 PM
To: 'Mc Ilvenny, Luke'
Subject: RE: CyberSecurity certificate budget review

Thank you, Luke. I appreciate your speedy review.

From: Mc Ilvenny, Luke [mailto:Luke.McIlvenny@oregonstate.edu]
Sent: Thursday, November 01, 2018 1:31 PM
To: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Subject: RE: CyberSecurity certificate budget review

Hi Chris,

I've reviewed the budget and it looks like it covers everything it needs to cover. I approve.

Regards,
Luke

From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Thursday, November 1, 2018 1:19 PM
To: Mc Ilvenny, Luke <Luke.McIlvenny@oregonstate.edu>
Cc: Ries, Carley W <carley.ries@oregonstate.edu>; Bromagem, Shaun <Shaun.Bromagem@oregonstate.edu>; Rampola, Corina A <corina.rampola@oregonstate.edu>
Subject: RE: CyberSecurity certificate budget review

Luke,

We've had a pleasant surprise. It turns out that we'll have enough manpower to update an online course that we hadn't anticipated being able to refresh (CS 373), as part of the cybersecurity certificate.

Consequently, I've had to update our budget to reflect the additional revenue and cost.

Sorry to ask this, but would you please be willing to review the updated version (attached) and provide feedback and/or approval?

Thank you in advance,
Chris

From: Mc Ilvenny, Luke [mailto:Luke.McIlvenny@oregonstate.edu]
Sent: Tuesday, October 30, 2018 10:41 AM
To: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Cc: Ries, Carley W <carley.ries@oregonstate.edu>; Bromagem, Shaun <Shaun.Bromagem@oregonstate.edu>; Rampola, Corina A <corina.rampola@oregonstate.edu>
Subject: RE: CyberSecurity certificate budget review

Hi Chris,

I have reviewed the budget and budget justification and find it to be complete and reasonably showing all expenses and revenues for the program. I approve this going forward to the Faculty Senate budget committee for final review.

Best of luck!
Luke

From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Tuesday, October 30, 2018 10:19 AM
To: Mc Ilvenny, Luke <Luke.McIlvenny@oregonstate.edu>; rampolac@onid.oregonstate.edu
Cc: Ries, Carley W <carley.ries@oregonstate.edu>; Bromagem, Shaun <Shaun.Bromagem@oregonstate.edu>
Subject: CyberSecurity certificate budget review

Luke and Corina,

I'm an associate professor helping my School of Electrical Engineering and Computer Science with a CAT I proposal that we hope to submit on Wednesday or Thursday. Shaun Bromagem, who helped us prepare the budget (attached), said that you are the right members of BEBC to contact for the required budget review.

Would you please be willing to review the attached documents and provide feedback and/or approval?

Thank you,
Chris Scaffidi
Associate Professor
College of Engineering

Capital Planning and Development
Oregon State University
3015 SW Western Blvd
106 Oak Creek Building
Corvallis, Oregon 97331

P 541-737-5412
F 541-737-4810
cpd.oregonstate.edu

11/2/2018

Christopher Scaffidi
Professor
School of Electrical Engineering and Computer Science
College of Engineering
3047 Kelly Engineering
Oregon State University
Corvallis, OR 97331

Dear Professor Scaffidi,

We appreciate the opportunity to review the School of Electrical Engineering and Computer Science proposal to offer a new Undergraduate Certificate in CyberSecurity. Per our review of the documentation provided and discussion, we understand that the program will require no immediate additional space to accommodate new faculty, instructional, research, student support and administrative functions.

From the Cat 1 proposal the additional space that is needed for this program will be found in the Civil and Construction Engineering space, and the additional office space for the new faculty members will be taken out of College of Engineering space.

Given that your proposal outlines a strategy for accommodating all of the current space needs within existing space assigned to the School of Electrical Engineering and Computer Science, Capital Planning and Development supports this proposal.

Sincerely,

Libby Ramirez
University Architect/Manager, Capital Resources
Oregon State University

Eric Smith
Management Analyst / Space Management
Oregon State University

Division of Extended Campus
Oregon State University
4943 The Valley Library
Corvallis, Oregon 97331

MOU Addendum for New Online and Portland Hybrid Certificate

Undergraduate Certificate in Cybersecurity

College of Engineering
Revised 1 Nov 2018

OSU Ecampus welcomes this opportunity to partner with the College of Engineering to make an Undergraduate Certificate in Cybersecurity available to an off-campus and Portland audience effective Summer 2019. This program will be an important addition to Oregon State's online offerings.

Partnership agreement

The following section provides a high-level overview of the partnership expectations of the College of Engineering, hereafter referred to as "the College", the support and services Ecampus provides, and the funding agreement.

Program coordination

The College agrees to ensure there is sufficient coordination of the program between the department and with Ecampus.

- The program coordination person(nel) are expected to be familiar with all sections of the MOU and ensure all agreed upon expectations have been met.
- Ecampus will fund the program development coordinator for three years.
- The College will identify the person(nel) responsible for coordination tasks. It is the responsibility of the academic unit to provide for ongoing administrative support for the program.

The College agrees to assign the following program development coordinator:

- Duties to be performed by Christopher Scaffidi, Associate School Head for Online and Continuing Education

Ecampus Support

Ecampus will assign an academic programs manager to be the key contact for the College regarding this program throughout its lifecycle. The academic programs manager will work with program personnel to coordinate efforts within Ecampus, through the curricular review/approval process, and thereafter. The academic programs manager will track program development progress and provide high-level reports to the College throughout the program's lifecycle. The College will ensure a continuous relationship with the academic programs manager and keep them informed of any impactful changes within the program.

Marketing and Enrollment Services (MES)

Whether it's through the Ecampus website, an inspiring story or a friendly phone call or email, the Ecampus Marketing and Enrollment Services team helps connect prospective online students with Oregon State.

- The Ecampus MES team will develop a program microsite (hosted on the Ecampus website) and will follow up with prospects through individualized and automated communications.

Course Development

Course	Developed on or before	PDX Hybrid (Offered)	Online (Offered)	Developer	Instructor
CS 370: Intro to Security	Fall 2018 & Winter 2019	Spring 2019	Summer 2019	Rakesh Bobba	Rakesh Bobba
CS 373: Defense Against the Dark Arts	Winter 2019 & Spring 2019	Summer 2019	Fall 2019	Kevin McGrath	Kevin McGrath
CS 427: Cryptography	Spring 2019 & Summer 2019	Fall 2019	Winter 2020	Mike Rosulek	Mike Rosulek
CS 478: Network Security	Spring 2019 & Summer 2019	Fall 2019	Winter 2020	Jesse Walker	Jesse Walker
CS 477: Digital Forensics	Summer 2019 & Fall 2019	Winter 2020	Spring 2020	Dave Nevin	Dave Nevin

Note: In addition to the courses above, the CyberSecurity certificate will include electives not part of this MOU, including several in existing computer science courses (e.g, CS 464, CS 492, CS 493, CS 496), as well as those being developed by the College of Business (BA 480 and BA 482). An addendum to this agreement will identify the course developers and funding amounts for the College of Business.

Course delivery

Ecampus provides scheduling and proctoring support for course delivery every term.

Term of Offer: Students may enroll in **Summer 2019**, or the earliest term permissible after CAT I approval by the Office of Academic Programs and Assessment**.**

Course scheduling: Ecampus schedules all online courses in coordination with the Office of the Registrar's schedule desk. To schedule a course, departments submit course CRN requests through the online CRN request form located on the Ecampus website at least two weeks before the first registration deadline of the upcoming term.

Proctored exams: The use of proctored exams for a course is at the discretion of the instructor and department. If proctored exams are going to be required, the CRN request should clearly indicate this. Ecampus Testing (ecampustesting@oregonstate.edu) will assist instructors and

students in locating and coordinating proctors and delivery of all exam materials. Ecampus Testing will also provide instructors with assistance for any special circumstances that might arise involving a proctored exam.

Program maintenance

A major factor in continued excellence is the maintenance and refreshment of courses and the program. As part of maintenance, the College commits to the following:

- Course redevelopment cycles every 3-5 years to ensure course material is current, relevant, and maintains curricular alignment (Ecampus has a proposal process and offers course development funding, training, and support for the redevelopment of courses.)
- Regular check-ins with program lead, coordinated through the Ecampus academic programs manager, to ensure marketing and recruitment, advising, student services, and course offerings are current and effective
- Communicate with Extended Campus' academic programs manager as changes to the program are being proposed, not post-facto
- Review program sustainability with Ecampus fiscal strategist

Total funding= $ 160,000

Course development

- **$ 75,000**
  - Funding provided per the schedule shown above.
  - Develop 5 new OSU courses (see Course Development, above) at $15,000 per course
  - The expectation that courses will be fully developed prior to the initial offer of the course.
  - Funds will be budget transferred to the College for support of course development:
    - once a course is deemed complete and up to standards, and
    - has been reviewed and approved by the appropriate designee of the College in collaboration with the Ecampus Director of Course Development and Training.

Program development coordinator

- **$75,000**
  - 3 years at .3FTE, Summer 2019 through Spring 2022
  - First payment of budget transferred to the department upon signing of the MOU;
  - Ecampus will assume no direct payroll.

Travel funding

- **$10,000**
  - Faculty/Instructor travel to be present in Portland hybrid course for instruction

Signatures

Signatures below indicate acceptance of these terms and conditions. Signatures also indicate that identified personnel (coordinators, advisors, course developers, Ecampus staff, etc.) will be notified of their responsibility in meeting the expectations outlined within this MOU.

DocuSigned by:
Belinda Batten
8A88062E62D3451...

11/7/2018 | 11:14:59 PST

Belinda Batten, College of Engineering
Executive Associate Dean

Date

DocuSigned by:
Carley Ries
51632BAEC70B4B3...

11/7/2018 | 10:10:47 PST

Carley Ries, College of Engineering
Assistant Dean of Online Learning

Date

DocuSigned by:
Lisa Templeton
F2AE947BBB704AC...

11/9/2018 | 08:49:27 PST

Lisa L. Templeton, Associate Provost
OSU Extended Campus

Date

Proposal for a New Academic Certificate Program

Proposal for the Initiation of a New Instructional Program Leading to an Undergraduate Certificate in CyberSecurity
Oregon State University
College of Engineering
School of Electrical Engineering and Computer Science
CPS Proposal #XXXXX
https://secure.oregonstate.edu/ap/cps/proposals/view/XXXXX

October 2018

1. Program Description

a. Proposed Classification of Instructional Programs (CIP) number

CIP Number: 11.1003
Title: Computer and Information Systems Security/Information Assurance.

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, programming, and systems analysis; networking; telecommunications; 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.

As computer systems have become part of the fabric of modern society, system security has ~~grown~~grown essential to the well-being of individuals, companies, the economy and life as we know it. A single security breach can expose the passwords[1], financial data[2] and most private personal information[3] of hundreds of millions of people. The total costs to companies has been estimated at $400 billion per year[4]. Worse yet, flaws in America's power grid control systems[5] and military systems[6] now put our national security at risk. In response, the National Institute of

[1] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[2] https://www.washingtonpost.com/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html
[3] https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html
[4] https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html
[5] https://nypost.com/2018/07/23/russian-hackers-could-have-caused-massive-power-outages
[6] https://www.theregister.co.uk/2018/10/15/us_military_weapn_system_vulnerabilities

Standards and Technology[7], the US Government Accountability Office[8], and the White House under Presidents Trump[9] and Obama[10] have all called for a greater emphasis on securing systems in government and in the private sector. Unfortunately, the worldwide shortage of cybersecurity professionals stands at 2.9 million at present[11], and, if current trends continue, will grow to 3.5 million by 2021[12]. The shortage of qualified workers has spiked the cost of hiring cybersecurity professionals, who earned an average salary of $116k[13] in 2017. Training the next generation of professionals in cybersecurity has thus become a civic duty of America's higher education system, as well as an economic opportunity for students interested in pursuing careers in technology.

In response, the College of Engineering proposes to establish a new Undergraduate Certificate in Cybersecurity. The proposed program will enable students to understand common threats to system security, assess security requirements for a new or existing system, implement secure solutions to counter threats, and evaluate systems to identify and address weaknesses. We expect these skills will enable students to obtain careers as cybersecurity professionals with job titles that include cybersecurity analyst, cybersecurity engineer, information assurance technician, and security administrator. In addition, these skills will enable students to perform other jobs, such as software engineer and requirements analyst, with a higher level of proficiency and a lower risk of creating security flaws that threaten their users, their employers, their livelihoods, and their nation.

---

[7] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[8] https://www.gao.gov/products/GAO-18-466
[9] https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/
[10] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf
[11] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[12] https://cybersecurityventures.com/jobs/
[13] https://www.cio.com/article/2383451/

Category	Information Summary
Proposal Title	Undergraduate Certificate in CyberSecurity
Proposal Purpose	New Undergraduate Certificate
Classification of Instructional Program (CIP) #	11.1003
Curriculum Proposal System # (incl link)	https://secure.oregonstate.edu/ap/cps/proposals/view/XXXX
Banner Student Information System (SIS) #	To be assigned by the Registrar's Office
Degree Type (e.g., B.S., M.S., or Ph.D.)	Not Applicable
Program Type (e.g., Undergraduate, Graduate, First Professional)	Undergraduate
Academic Home	College of Engineering
College Code	16
Contacts (e.g,, Name, Title, Tel #, eMail Address)	Dr. Carlos Jensen Associate Dean 541-737-2555 carlos.jensen@oregonstate.edu
Faculty (New)	No new faculty required for certificate launch
Staff (New)	No new staff required for certificate launch
Library (New)	No new resources required for certificate launch
Facilities/Space (New)	No new buildings required for certificate launch
Budget (first four years)	See budget worksheet
Undergraduate Option(s)	Not Applicable

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

Course	Credits	Title	Notes
CS 370	4	Introduction to Security	
CS 373	4	Defense against the Dark Arts	
CS 427	4	Cryptography	
CS 477	4	System Security	Already exists as CS 419 (special topic) and will get its own number
CS 478	4	Network Security	
Electives	7	Any 400-level courses in Computer Science or College of Business	

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).

We propose to offer courses for this certificate at the frequencies, modalities and locations shown below. Asterisks * indicate course modalities that already will be in place at the time of this certificate program's launch; these include CS 370 and CS 373, which are currently under a separate CAT II proposal (expected to be approved prior to this CAT I proposal). Carets ^ indicate course modalities that we will create (by adapting existing courses) as part of the certificate program's launch.

Course	In-person in Corvallis	Hybrid via Ecampus + Portland (Meier Frank Building)	Online via Ecampus
CS 370	Once per year *	Once per year *	Every term *
CS 373	Once per year *	Once per year *	Every term *
CS 427	Once per year *	Once per year ^	Every term ^
CS 477	Once per year *	Once per year ^	Every term ^
CS 478	Once per year *	Once per year ^	Every term ^
Electives	Most are offered at least once per year *	Some may be offered once or twice per year *	Most available online are offered every term *

Given sufficient demand, we might increase the hybrid offerings to twice per year.

To satisfy the 7 elective credit hours of the certificate, students may choose from a wide range of available courses. Examples of courses taught every year in Corvallis, and every term via Ecampus, include the following:

- CS 434 - Machine Learning and Data Mining (4 credits)
- CS 464 - Open Source Software (4 credits)
- CS 475 - Intro to Parallel Programming (4 credits)
- CS 493 - Cloud Application Development (4 credits)

Such courses provide venues for applying concepts from cybersecurity. For example, the Open Source Software course (CS 464) includes a learning outcome that involves contributing to an existing open source project, which for a student interested in cybersecurity could involve contributing a security fix to an existing project. Students more interested in satisfying the elective with courses courses from the College of Business will also find ample opportunity for applying their knowledge of cybersecurity on the business side of diverse technologies. For example, Business Analytics (BA 483) covers RFID tags and social networks, Information Systems Security (BA 480) covers identity management and management of physical security, and Business Telecom and Networking (BA 479) focuses on the five-layer internet model as it pertains to business environments. We are confident that every student interested in cybersecurity will find a broad range of acceptable choices for satisfying the electives. Once we have observed which courses enjoy the largest popularity with students, we will likely file a CAT II to add a hybrid modality to that subset of courses.

e. Ways in which the program will seek to assure quality, access, and diversity.

Student qualifications: We will review all applications to ensure that applicants are currently pursuing a Bachelor's degree at Oregon State University, have a GPA of at least 3.0, and obtained at least a C in the prerequisite courses of our required courses (i.e., CS 261 Data Structures, CS 340 Introduction to Databases, CS 344 Operating Systems, and CS 372 Computer Networking). Revise if Carley finds a way for non-BS students to enroll.

Access: In order to increase the availability of the certificate to students who might take a non-traditional track through their education, we will allow applicants with 3+ years of professional experience as software or system engineers to petition for the waiver of one or more prerequisite. Decisions regarding waivers will be made at the discretion of instructors.

Student success: Our School's academic advisors[14] will be available on-demand to guide existing BS students regarding appropriateness of the certificate for their career goals, to help students select career-relevant electives, and to coach struggling students. A team of 4-5 Ecampus advisers and coaches[15] guide students on following policies, obtaining exam proctors, setting goals, managing time, and similar student-success topics.

[14] http://eecs.oregonstate.edu/current-students/undergraduate/advising
[15] https://ecampus.oregonstate.edu/services/student-services/

Diversity: We designed the electives component of our curriculum with the intention of accommodating the diverse interests of students, with a particular focus on students who may be pursuing a business major and a minor in computer science (e.g., with the intention of ultimately pursuing a career in management at a technology company). We also hope to accommodate students from diverse backgrounds, including those residing in Portland's urban setting, by offering our curriculum via a range of modalities and locations. Furthermore, we anticipate that the availability of evening courses in the Meier Frank / Portland location will aid in accommodating the needs of students who cannot afford to stop working while going to school and who therefore must schedule courses around job-related constraints.

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

We expect approximately 12-18 to enroll in the program each year. It's probable that we will be at the lower end of that range in the first year but grow toward the upper end by the fifth year.

Academic year	Est. Headcount	Est. FTE
2019-20	12-18	7.5
2020-21	12-18	7.5
2021-22	12-18	7.5
2022-23	12-18	7.5
2023-24	12-18	7.5

g. Expected degrees/certificates produced over the next five years.

We expect that each student will typically complete the certificate in one year. At 15 per year, our 5-year projection is 75 certificate completions.

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

TODO. Write this based on whether Carley finds a way for non-BS students to enroll.

i. Adequacy and quality of faculty delivering the program.

The team leading, developing and delivering the first year of our program includes the following:

- Chris Scaffidi: PhD in Software Engineering; Associate School Head in OSU's School of Electrical Engineering and Computer Science; Associate Professor; has created 3 of the core 15 courses in our Computer Science Post-Bacc program; has taught and researched software engineering and other computer science topics at OSU for 9 years; has served as

school liaison to the Technology Association of Oregon; has worked previously for 6 years as a professional software engineer.

- Rakesh Bobba: PhD in Electrical and Computer Engineering; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched security and other computer science topics at OSU and the University of Illinois for 9 years; has served as Co-PI for multiple federally-funded cybersecurity projects; serves on the Oregon Cybersecurity Advisory Council, established in 2017 to advise the State Chief Information Officer on cybersecurity matters and to develop a shared vision for the establishment of a cross-sector Cybersecurity Center of Excellence
- Mike Rosulek: PhD in Computer Science; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched cryptography and other computer science topics at OSU and the University of Montana for 9 years; has an internationally-recognized reputation as a cryptographer; has helped to lead the International Association for Cryptologic Research.
- Yeongjin Jang: PhD in Computer Science; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched ethical hacking and other computer science topics at OSU for 1 year; has won the highly-coveted Black Badge award from DEF CON in 2015 and 2018; placed as finalist in the DARPA Cyber Grand Challenge in 2016.
- Jesse Walker: PhD in Mathematics; Research Professor in the School of Electrical Engineering and Computer Science; previously was Intel's Chief Cryptographer; has collaborated on research and development of security-related aspects of system design for approximately two decades; achieved international impact for discovering a key weakness in what was the most widely-used wireless protocol (WEP), as well as for helping to invent replacement protocols (WPA and WPA2) now in widespread use.
- Kevin McGrath: MS in Computer Science; Senior Instructor in the School of Electrical Engineering and Computer Science; also Security Researcher at McAfee Advanced Threat Research Lab; has taught and researched operating system design and security, as well as other computer science topics, at OSU for 7 years

j. Faculty resources – full-time, part-time, adjunct.

The first four faculty above are full-time (but will work part-time on leading our proposed certificate program), while the last two are part-time.

k. Other staff.

The certificate program will be supported by existing staff in the School of Electrical Engineering and Computer Science and in Ecampus. These include:

- The Associate School Head for Online Programs (Section 1.i) will inform and oversee creation of courses for the hybrid and online modalities, as well as lead the evaluation of the program and its teachers.
- The Admissions Coordinator will review student applications per the criteria above (Section 1.e)

- Academic Advisers, including 3-4 in the School plus 4 in Ecampus, together will serve our existing student population both on-campus and online to promote student success (Section 1.e).
- At least one 0.49 FTE graduate Teaching Assistant per course, in addition to two 0.49 FTE "pool TAs" dedicated to serving our Ecampus and hybrid students across all courses in the Portland area, will hold weekend office hours downtown.

l. Facilities, library, and other resources.

The current facilities, library and other resources will adequately support the proposed certificate.

m. Anticipated start date.

Summer 2019

2. Relationship to Mission and Goals

a. Manner in which the proposed program supports the institution's mission and goals for access; student learning; research, and/or scholarly work; and service.

Security flaws can harm individual consumers worldwide, as well as Oregonian companies and others that sell affected software. Mistakes that affect military systems, electricity infrastructure, and other mission-critical systems can even threaten the national security of the United States. Therefore, offering a new certificate in the high-impact area of cybersecurity will align with the university's commitment to promote the well-being of Oregon, the nation and the world. Moreover, the proposed certificate will support the university's education mission by preparing students for obtaining jobs in cybersecurity-related careers.

b. Connection of the proposed program to the institution's strategic priorities and signature areas of focus.

Establishing a technically proficient workforce is essential to Oregon's economic development, and it ties directly to the Healthy Economy strategic priority of OSU.

c. Manner in which the proposed program contributes to Oregon University System goals for access; quality learning; knowledge creation and innovation; and economic and cultural support of Oregon and its communities.

Section 1.e discusses in detail how different aspects of the proposed program will contribute to quality learning, access, and diversity. Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

d. Manner in which the program meets broad statewide needs and enhances the state's capacity to respond effectively to social, economic, and environmental challenges and opportunities.

Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

3. Accreditation

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

We are not aware of any accrediting body or professional society that has established standards for cybersecurity education, although several companies and societies offer certifications of their own for different subsets of cybersecurity. The closest standard that spans all of our potential students' interest areas is from NIST's National Initiative for Cybersecurity Education (NICE); specifically, this NICE Cybersecurity Workforce Framework[16] characterizes the ways in which different cybersecurity professions are similar or different in terms of the capabilities required of professionals.

We used this framework, as well as a review of the diverse career directions that we anticipate students may take, to identify a core of technical knowledge and skills essential to a range of different career paths. We then incorporated these desirable student capabilities as learning outcomes in the 5 required courses of the proposed certificate. Finally, we designed the proposed certificate to require students to pursue additional electives in an area relevant to their long-term career interests.

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.

Not applicable

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

[16] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

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.

Not applicable because we are not aware of any accrediting body for cybersecurity education.

4. Need

a. Evidence of market demand.

As described in Section 1.a, millions of high-paying jobs in cybersecurity are going unfilled. Relevant statistics include:

- 2.9 million unfilled positions estimated in 2018[17]
- 3.5 million unfilled positions projected in 2021[18]
- Growth rate forecast at 37% from 2012-2022[19]
- Average salary $116k in 2017[20]
- Entry level salary $66k in 2018[21]
- Steep payscale, rising to $233k for chief information security officers in 2018[22]

The underlying source of market demand for cybersecurity professionals is the burgeoning number of massive, expensive security flaws. Relevant statistics include:

- 5,000 publicly revealed breaches in 2017[23]
- 189,445 total known security vulnerabilities in commercial software since 2011, including 17,091 in 2018[24]
- Over 19 billion records affected in total from known breaches between 2015-2018[25]
- Average cost of $7.3M per security breach in the United States in 2017[26]
- $4.7B projected revenue for digital forensics firms (alone) in 2020[27]

As long as the pace and impact of security breaches continues to accelerate, market demand for cybersecurity professionals will likely remain strong, as well.

---

[17] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[18] https://cybersecurityventures.com/jobs/
[19] https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs
[20] https://www.cio.com/article/2383451/
[21] https://tinyurl.com/payscale-entry-level-cyber-sec
[22] https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000
[23] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[24] https://vulndb.cyberriskanalytics.com/
[25] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[26] https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html
[27] https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html

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

c. Manner in which the program would serve the need for improved educational attainment in the region and state.

We anticipate that the certificate will help students to advance in their current job or to obtain a more preferred job where they can use their new skills.

d. Manner in which the program would address the civic and cultural demands of citizenship.

As noted in Section 1.a, security flaws threaten the well-being of companies, individuals, and our nation. Because of the urgent risk to so many aspects of modern society, we feel that all of the required courses of our proposed program include learning outcomes relevant to civic and cultural life. To illustrate, consider the first two of our required courses...

- CS 370 - Introduction to Security: This course teaches students about typical threats to privacy, security, accountability and similar fundamental attributes that we take for granted in the systems that pervade everyday life. The course thereby enables students to achieve the learning outcome to "Understand the need for cyber security, key notions of security, and well established security principles and security mechanisms/controls."
- CS 373 - Defense against the Dark Arts: This course teaches students in further detail about threats to security in modern society, so that they can "Demonstrate awareness of the current state of malware, adware, and crypto-ware." Furthermore, it teaches techniques to counter these threats. For example, two other learning outcomes are that students can "Implement spam identification tools" and can "Implement solutions to common attack vectors in multiple environments." The course thus teaches students how to protect against the malware that frequently takes over peoples' computers, against the spam that chokes their communications, and against the crypto-ware that encrypts the hard drives of consumers and companies (then demands a ransom).

5. Outcomes and Quality Assessment

a. Expected learning outcomes of the program.

Students completing the proposed certificate program will be able to:

- Describe the common threats to system security and explain their mechanisms of action
- Assess the security requirements for a proposed or existing system
- Implement secure solutions to common threats by selecting and applying appropriate principles, protocols and techniques.

- Evaluate system designs, implementations and protocols to identify and ameliorate weaknesses

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

Every other spring, our school's Associate School Head for Online and Continuing Education will email students enrolled in the certificate, inviting them to complete a questionnaire about their perception of what they have learned related to the program learning outcomes. This questionnaire will be designed with the input of the courses' instructors and, for each of the 4 program learning outcomes, will aim at uncovering what elements of specific courses were most helpful in achieving that learning outcome. Then, learning outcomes will be identified for which few if any course elements were relevant or beneficial. The Associate School Head will then collaborate with the instructors to identify and implement strategies for improving the curriculum during the subsequent year. Then, in the following year, the next round of questionnaires will make it possible to assess the extent to which these changes improved student outcomes.

c. Program performance indicators, including prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate.

The College of Engineering performs a yearly survey of recent BS graduates using a questionnaire similar to that of the National Association of Colleges and Employers (NACE) First-Destination Survey. Our college will augment this survey with new questions enabling us to measure the percent of certificate graduates who report obtaining a job that involves designing, implementing, troubleshooting or managing security-related aspects of systems. These questions will already part of the survey deployed prior to the graduation of our first cohort of students in the certificate program, thereby providing us a baseline for comparison when judging whether our program aids students in obtaining measurably better career outcomes. In addition, these questions will be part of the survey given to all computer science graduates in the future, enabling us to assess whether students graduating with our certificate achieve better career outcomes on our target metric than students lacking the certificate.

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

The College of Engineering has established expectations for the nature and level of research and/or scholarly activity of faculty. The School of Electrical Engineering and Computer Science evaluates all tenure/tenure-track faculty on an annual basis to ensure they meet expectations, and the College of Engineering reviews all faculty considered for tenure and promotion. The proposed certificate will not impact any of these expectations for research and/or scholarly work.

6. Program Integration and Collaboration

a. Closely related programs in other OUS universities and Oregon private institutions.

Several Oregon institutions offer somewhat topically-related initiatives.

- Oregon Institute of Technology (OIT) operates a Cyber Defense Center, within which students learning cybersecurity can practice on companies facing security issues. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[28]
- Portland State University (PSU) has hosted GenCyber summer camps for high schoolers. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[29]
- Mt. Hood Community College (MHCC) offers an Associate of Applied Science in Information Systems and Technology Management in Cyber Security and Networking. The program focuses on hardware- and networking-related aspects of security. It is therefore less broad than our proposed certificate program, which will address hardware, network, software, protocol, mathematical and management aspects of system security.[30]

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.

After our certificate program has gotten established, collaborating with the programs above could provide avenues for expanding student headcount and program impact. For example, PSU actively recruits other organizations (including universities) to host their summer camps; serving as a PSU GenCyber camp could enable OSU to more effectively reach seniors in high school, as a means of exciting them about applying to OSU to study cybersecurity further.

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

See 6.b above. We believe that establishing a cybersecurity certificate will enhance our credibility as a potential partner to other organizations and open up opportunities for collaboration.

d. Potential impacts on other programs in the areas of budget, enrollment, faculty workload, and facilities use.

None anticipated.

[28] https://www.oit.edu/cyber-defense-center
[29] https://www.gen-cyber.com/
[30] https://www.mhcc.edu/CyberSecurityNetworkingCurriculum/

7. Financial Sustainability (attach Budget Outline)

a. Business plan for the program that anticipates and provides for its long-term 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.

Existing school staff supporting our existing programs will suffice for offering the certificate program. The curriculum will adapt existing courses, and our college has budgeted for this one-time expense. Faculty for teaching the certificate's program through the first year have already been identified, and a standing hiring committee has been established to continually accept and evaluate applications for positions as instructors across all teaching modalities and locations (Corvallis in-person courses, Ecampus online courses, and Portland hybrid courses). We do not anticipate any significant new demands on library resources.

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

None anticipated.

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

To obtain their required 27 credit-hours for the proposed certificate, students will typically take 7 courses, which approximately equals the number of sections taught by a 1.0 FTE instructor in our college. Because we project certificate demand at 15 students (7.5 FTE) per year, we therefore target a 7.5 student:faculty FTE ratio. We do not anticipate an impact on class sizes because the college is moving toward a model of splitting classes to keep section sizes at or just below 50 students each; this target is consistent with results from a review of the literature[31], as well as specific studies in other fields indicating that such sizes offer meaningful cost savings over smaller courses[32], potentially with little or no negative impact on student outcomes relative to smaller courses[33,34] and that students consider class sizes approximately between 20 and 40 to promote meaningful peer interaction[35].

---

[31] Taft, S. H., Perkowski, T., & Martin, L. S. (2011). A framework for evaluating class size in online education. *The Quarterly Review of Distance Education, 12*(3).

[32] Bettinger, E., Doss, C., Loeb, S., Rogers, A., & Taylor, E. (2017). The Effects of Class Size in Online College Courses: Experimental Evidence. *Economics of Education Review*.

[33] Gorman, C., Webb, D., & Gee, K. (2018). Hierarchical Linear Modeling Approach to Measuring the Effects of Class Size and Other Classroom Characteristics on Student Learning in an Active-Learning Based Introductory Physics Course. arXiv preprint arXiv:1809.00218. https://arxiv.org/ftp/arxiv/papers/1809/1809.00218.pdf

[34] Monks, J. & Schmidt, R. (2011). The Impact of Class Size on Outcomes in Higher Education. *The B.E. Journal of Economic Analysis & Policy, 11*(1), doi:10.2202/1935-1682.2803.

[35] Burruss, N., Billings, D., Brownrigg, V., Skiba, D., & Connors, H. (2008). Class Size as Related to the Use of Technology, Educational Practices, and Outcomes in Web-Based Nursing Courses. *Journal of Professional Nursing*. DOI: https://doi.org/10.1016/j.profnurs.2008.06.002

d. Resources to be devoted to student recruitment.

The College of Engineering has budgeted for a marketing campaign to be conducted in partnership with Ecampus, as a means of highlighting our Portland presence and the availability of our proposed certificate.

8. External Review (if the proposed program is a graduate level program)

Not applicable

Christopher Scaffidi

From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Wednesday, October 24, 2018 2:57 PM
To: 'Reitsma, Reindert F'
Cc: 'Swift, Michele - COB'
Subject: RE: Cyber CAT1

Hi, Rene,

That makes sense -- I hadn't understood all the factors that went into your preferred design. I'll edit the proposal to specify that the only COB courses allowed to satisfy the elective are 480 and 482 (in addition to CS, of course).

Thank you for taking the time to explain.

Chris

From: Reitsma, Reindert F [mailto:reitsmar@bus.oregonstate.edu]
Sent: Wednesday, October 24, 2018 2:51 PM
To: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Cc: Swift, Michele - COB <michele.swift@bus.oregonstate.edu>
Subject: RE: Cyber CAT1

Chris, see answers in red below

From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Wednesday, October 24, 2018 2:23 PM
To: Reitsma, Reindert F <reitsmar@bus.oregonstate.edu>
Subject: FW: Cyber CAT1

Rene,

Thank you for all the helpful suggestions, which I have incorporated.

You asked about whether we could tell students that they only may satisfy the elective with CS courses, or with BA 480 and/or 482 (rather than any 400-level CS or COB course). From my standpoint, I like the idea of letting students draw upon the broader range of great courses that COB offers, where students could apply their cybersecurity knowledge. For example, Business Analytics (BA 483) covers RFID tags and social networks, and Business Telecom and Networking (BA 479) focuses on the five-layer internet model as it pertains to business environments. Perhaps we could compromise and let students choose from CS or from BA 479, 480, 481, 482, and 483? (It's nice that all of these technology-focused courses have such similar numbers; did you plan this?)

Nonetheless, if you feel strongly, I can make your suggested change and eliminate the option to take other BA courses besides 480 and 482. Is that what you'd prefer?
I think that we'd prefer them to take the BA482 course (or BA480) because we are preparing this especially for the Certificate program. I believe that it was the intention of the CS faculty (ask Carley) to even make BA482 a required course, but that this could not be specified at this time because the course had not yet made its way through the CPS.

On a different note: it took me (and a few of my colleagues) some effort to get this going and I would not like it one bit if students would now ignore it and take some other business course. Also, almost all Business 400-level classes (other than special ones such as self-directed courses, internship courses, etc.) have business prereqs on them.

Also, would making that change in any way delay or slow the CAT I approval process, due to the fact that BA482 is new and hasn't yet been approved?
Well, that's the real question. I think that's why Carley did it the way she did it.

Thanks,
Chris

From: Reindert F Reitsma (Google Docs) [mailto:d+MTE0MjMyODk2ODIzNDgzODAwNjcz-MTAyNTQyNjQwNzEzOTYzMTg0MTM5@docs.google.com]
Sent: Wednesday, October 24, 2018 1:09 PM
To: Scaffidi, Christopher Paul <Christopher.Scaffidi@oregonstate.edu>
Subject: Cyber CAT1

Reindert F Reitsma added comments and suggestions to Cyber CAT1
New

1 comment, 8 suggestions

New

Comments

Reindert F Reitsma

We do not anticipate an impact on class sizes because the college is moving toward a model of splitting classes to keep section sizes at or just below 50 students each; this target is consistent with results from a review of the literature, as well as specific studies in other fields indicating that such sizes offer meaningful cost savings over smaller courses, potentially with little or no negative impact on student outcomes relative to smaller courses, and that students consider class sizes approximately between 20 and 40 to promote meaningful peer interaction.

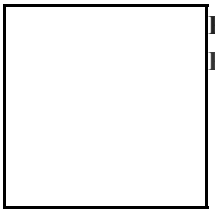
This is one hell of a long and awkward sentence. I suggest reformulating it into several ones.

ReplyOpen

Suggestions

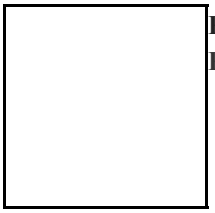
Reindert F Reitsma
Replace: *"gotten"* with *"been"*

ReplyOpen



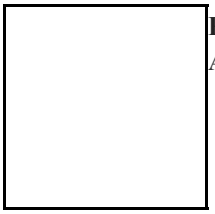
Reindert F Reitsma
Replace: *"less broad"* with *"narrower"*

ReplyOpen



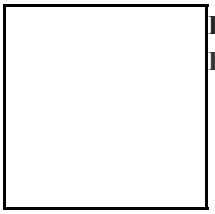
Reindert F Reitsma
Replace: *"judging"* with *"assessing"*

ReplyOpen



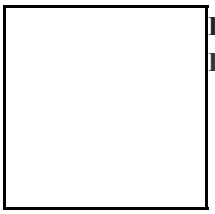
Reindert F Reitsma
Add: *"be"*

ReplyOpen



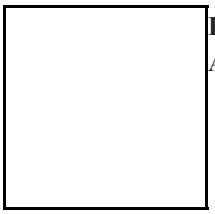
Reindert F Reitsma
Replace: *"us"* with *"it"*

ReplyOpen



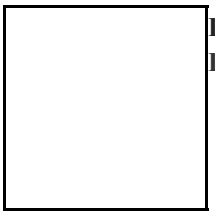
Reindert F Reitsma
Replace: *"Our"* with *"The"*

ReplyOpen



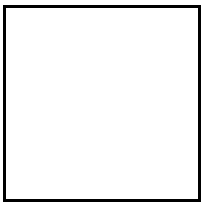
Reindert F Reitsma
Add: *"and least"*

ReplyOpen



Reindert F Reitsma
Replace: *"student"* with *"learning"*

ReplyOpen



Proposal for a New Academic Certificate Program

Proposal for the Initiation of a New Instructional Program Leading to an Undergraduate Certificate in CyberSecurity
Oregon State University
College of Engineering
School of Electrical Engineering and Computer Science
CPS Proposal #105390
https://secure.oregonstate.edu/ap/cps/proposals/view/105390

October 2018

1. Program Description

a. Proposed Classification of Instructional Programs (CIP) number

CIP Number: 11.1003
Title: Computer and Information Systems Security/Information Assurance.

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, programming, and systems analysis; networking; telecommunications; 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.

As computer systems have become part of the fabric of modern society, system security has grown essential to the well-being of individuals, companies, the economy and life as we know it. A single security breach can expose the passwords,[1] financial data[2] and private personal information[3] of hundreds of millions of people. According to the Lloyd's insurance company, hacking costs businesses an estimated annual total of $400 billion worldwide, "including the damage itself and subsequent disruption to the normal course of business."[4] Worse yet, flaws in America's power-grid control systems[5] and military systems[6] now put national security at risk. In response, the National Institute of Standards and Technology,[7] the US Government Accountability Office,[8] and the White House under Presidents Trump[9] and Obama[10] have all called for a greater emphasis on securing systems in government and in the private

[1] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[2] https://www.washingtonpost.com/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html
[3] https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html
[4] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/
[5] https://nypost.com/2018/07/23/russian-hackers-could-have-caused-massive-power-outages
[6] https://www.theregister.co.uk/2018/10/15/us_military_weapn_system_vulnerabilities
[7] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[8] https://www.gao.gov/products/GAO-18-466
[9] https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/
[10] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf

sector. Unfortunately, the worldwide shortage of cybersecurity professionals stands at 2.9 million at present[11] and, if current trends continue, will grow to 3.5 million by 2021.[12] The shortage of qualified workers has increased the cost of hiring cybersecurity professionals, who earned an average salary of $116k in 2017.[13] Training the next generation of professionals in cybersecurity has thus become a civic duty for America's higher education system, as well as an economic opportunity for students interested in pursuing careers in cybersecurity-related technology.

In response, the College of Engineering proposes to establish a new Undergraduate Certificate in Cybersecurity. The proposed program will enable students to understand common threats to system security, assess security requirements for a new or existing system, implement secure solutions to counter threats, and evaluate systems to identify and address weaknesses. It expected that these skills will enable students to obtain careers as cybersecurity professionals with job titles that include cybersecurity analyst, cybersecurity engineer, information assurance technician, and security administrator. In addition, these skills will enable students to perform other jobs, such as software engineer and requirements analyst, with a higher level of proficiency and a lower risk of creating security flaws that threaten their users, their employers, their livelihoods, and their nation.

[11] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[12] https://cybersecurityventures.com/jobs/
[13] https://www.cio.com/article/2383451/

Category	Information Summary
Proposal Title	Undergraduate Certificate in CyberSecurity
Proposal Purpose	New Undergraduate Certificate
Classification of Instructional Program (CIP) #	11.1003
Curriculum Proposal System # (incl link)	https://secure.oregonstate.edu/ap/cps/proposals/view/105390
Banner Student Information System (SIS) #	To be assigned by the Registrar's Office
Degree Type (e.g., B.S., M.S., or Ph.D.)	Not Applicable
Program Type (e.g., Undergraduate, Graduate, First Professional)	Undergraduate
Academic Home	College of Engineering
College Code	16
Contacts (e.g,, Name, Title, Tel #, eMail Address)	Dr. Carlos Jensen, Associate Dean 541-737-2555 carlos.jensen@oregonstate.edu
Faculty (New)	No new faculty required for certificate launch
Staff (New)	No new staff required for certificate launch
Library (New)	No new resources required for certificate launch
Facilities/Space (New)	No new buildings, office or labs required for certificate launch
Budget (first four years)	See budget worksheet
Undergraduate Option(s)	Not Applicable

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

Course	Credits	Title	Notes
CS 370	4	Introduction to Security	Existing course to be adapted for alternate modalities; see CAT II in CPS
CS 373	4	Defense Against the Dark Arts	Existing course to be adapted for alternate modalities; see CAT II in CPS
CS 427	4	Cryptography	Existing course to be adapted for alternate modalities; see CAT II in CPS
CS 477	4	Digital Forensics	New course to be created for all modalities; see CAT II in CPS
CS 478	4	Network Security	Existing course to be adapted for alternate modalities; see CAT II in CPS
Electives	7	BA 480, BA 482, CS 434, CS 464, CS 475, CS 492, CS 493, CS 496	
TOTAL	**27**		

To satisfy the 7 elective credit hours of the proposed undergraduate certificate program, students will have many choices. Applicable computer science courses taught every year in Corvallis, and every term via Ecampus, include the following:

- CS 434 - Machine Learning and Data Mining (4 credits)
- CS 464 - Open Source Software (4 credits)
- CS 475 - Intro to Parallel Programming (4 credits)
- CS 492 - Mobile Software Development (4 credits)
- CS 493 - Cloud Application Development (4 credits)
- CS 496 - Mobile/Cloud Development (4 credits) [will be phased out, replaced by 492/493]

Such courses provide venues for applying concepts from cybersecurity. For example, the Open Source Software course (CS 464) includes a learning outcome that involves contributing to an existing open source project, which for a student interested in cybersecurity could involve contributing a security fix to an existing project. They will be available via Ecampus (and in Corvallis) to all students in the program.

Students may also select from either Information Systems Security (BA 480) or Information Systems Governance (BA 482, for which the College of Business currently is preparing a CAT II proposal). The College of Business has specifically identified these courses as being of potential interest to students interested in business aspects of cybersecurity.

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).

Courses for the proposed certificate program will be offered at the frequencies, modalities and locations shown below.

Course	In-person in Corvallis	Hybrid via Ecampus + Portland (Meier & Frank Building)	Online via Ecampus
CS 370	Once per year	At least once per year	At least once per year
CS 373	Once per year	At least once per year	At least once per year
CS 427	Once per year	At least once per year	At least once per year
CS 477	Once per year	At least once per year	At least once per year
CS 478	Once per year	At least once per year	At least once per year
Electives	Most are offered at least once per year	Some may be offered once or twice per year	Most available online are offered every term

Given sufficient demand, the frequency of hybrid offerings might increase up to twice per year, and that of online offerings might increase up to every term. This will depend not only on the number of students enrolled in the proposed undergraduate certificate program itself (section f, below), but also on the number of other students who want to take the courses.

All five required courses of the proposed certificate program will require course-preparation for the hybrid modality; refer to the Curriculum Proposal System for each course's corresponding CAT II proposal. All of these required courses already exist for the in-person modality (at the Corvallis campus) except CS 477, which will be a new course.

e. Ways in which the program will seek to assure quality, access, and diversity.

Even though it is anticipated at present that almost all students enrolling in the proposed certificate program will be enrolled in the Bachelor's or Post-Baccalaureate degree programs in *computer science*, other students are anticipated to be enrolled in a *business-related* undergraduate program. Longer-term, it is possible that students pursuing undergraduate degrees in *other* fields might also wish to obtain a certificate in cybersecurity. The reason is that cybersecurity is becoming an important issue in civil engineering,[14] smart manufacturing,[15] farming,[16] political science,[17] and a broad range of other fields. All undergraduate students will be welcome to pursue the proposed cybersecurity certificate, provided that they are adequately qualified (as defined below).

Although, at present, OSU only allows students concurrently seeking an undergraduate degree to register for an undergraduate certificate, this policy is currently under revision at the university level to permit a new application admissions procedure for qualified students to enroll in certificate programs. Until OSU establishes that new procedure, the proposed certificate program will only enroll students concurrently pursuing an undergraduate degree. Once OSU has established a procedure for students to enroll directly in undergraduate certificate programs, then qualified students will also be able to enroll in the proposed cybersecurity undergraduate certificate program.

[14] https://www.afcec.af.mil/News/Article-Display/Article/1319284/
[15] https://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/
[16] https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data
[17] https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/

Student qualifications: The School of Electrical Engineering and Computer Science will review all applications to ensure that applicants are concurrently pursuing an undergraduate degree at Oregon State University, have a GPA of at least 3.0, and have obtained at least a C in the prerequisite courses of the required degree program courses (i.e., CS 261 Data Structures, CS 340 Introduction to Databases, CS 344 Operating Systems, and CS 372 Computer Networking). As noted above, the University anticipates eventually allowing students to enroll directly into undergraduate certificate programs (i.e., without concurrently seeking an undergraduate degree); such students will still need to meet the GPA and the prerequisite requirements, above (in addition any university-level requirements on such students).

Access: In order to increase the availability of the proposed certificate program to students who might take a non-traditional track through their education, applicants with 3+ years of professional experience as software or system engineers will be allowed to petition for the waiver of one or more prerequisites. Decisions regarding waivers will be at the discretion of instructors.

Student success: The School's academic advisors[18] will be available on-demand to guide potential students regarding appropriateness of the proposed certificate program for their career goals, to help students select career-relevant electives, and to coach struggling students. A team of 4-5 Ecampus advisers and coaches[19] guide students on following policies, obtaining exam proctors, setting goals, managing time, and similar student-success topics.

Diversity: The College of Engineering, in coordination with the College of Business, designed the electives component of the curriculum with the intention of accommodating the diverse interests of students, with a particular focus on students who may be pursuing a major in business or another field (e.g., with the intention of ultimately pursuing a career in management at a technology company). The proposed program will accommodate students from diverse backgrounds, including those residing in Portland's urban setting, by delivering the curriculum via a range of modalities and locations. Furthermore, it is anticipated that the availability of evening courses in the Portland satellite facility location will aid in accommodating the needs of students who cannot afford to stop working while going to school and who therefore must schedule courses around job-related constraints.

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

Approximately 12-18 students are expected to enroll each year. The number will probably start at the lower end of that range in the first year, then grow toward the upper end by the fifth year.

Academic year	Estimated Headcount	Estimated FTE	Cumulative Est. Completions
2019-20	12	6	12
2020-21	14	7	26
2021-22	15	7.5	41
2022-23	16	8	57
2023-24	18	9	75

[18] http://eecs.oregonstate.edu/current-students/undergraduate/advising
[19] https://ecampus.oregonstate.edu/services/student-services/

g. Expected degrees/certificates produced over the next five years.

Each student will typically complete the proposed undergraduate certificate program in one year. If an average of 15 complete the proposed certificate program per year during the first five years, as expected, then a total of 75 will complete the proposed certificate program by the end of that period (see table above).

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

The program will primarily serve students concurrently pursuing an undergraduate degree (as noted above in section e). Most of the students are expected to be traditional, resident, full-time students pursuing a Bachelor's degree in computer science at the Corvallis campus. A smaller group of students will be non-traditional students pursuing the Post-Baccalaureate Bachelor's degree in computer science (generally part-time via Ecampus), some of whom will live in the Portland area; others will be non-residents. A still smaller group of students are expected to be traditional, resident, full-time students pursuing a Bachelor's degree in a business field with a minor or an interest in computer science. It is expected that in the longer-term, some students from other fields might wish to enroll in the proposed certificate program (as noted in section e), though this is speculative at present. Eventually, once OSU has established a procedure for enrolling directly into undergraduate certificates without a concurrent degree program, the proposed cybersecurity certificate program is expected to serve software engineers in the Portland area (as part-time students via Ecampus and/or hybrid courses at the Portland satellite).

i. Adequacy and quality of faculty delivering the program.

The team leading, developing and delivering the first year of the program includes the following:

- Chris Scaffidi: PhD in Software Engineering; Associate School Head in OSU's School of Electrical Engineering and Computer Science; Associate Professor; has created 3 of the core 15 courses in the Computer Science Post-Bacc program; has taught and researched software engineering and other computer science topics at OSU for 9 years; has served as school liaison to the Technology Association of Oregon; has worked previously for 6 years as a professional software engineer.
- Rakesh Bobba: PhD in Electrical and Computer Engineering; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched security and other computer science topics at OSU and the University of Illinois for 9 years; has served as Co-PI for multiple federally-funded cybersecurity projects; serves on the Oregon Cybersecurity Advisory Council, established in 2017 to advise the State Chief Information Officer on cybersecurity matters and to develop a shared vision for the establishment of a cross-sector Cybersecurity Center of Excellence.
- Mike Rosulek: PhD in Computer Science; Assistant Professor in the School of Electrical Engineering and Computer Science; has taught and researched cryptography and other computer science topics at OSU and the University of Montana for 9 years; has an internationally-recognized reputation as a cryptographer; has helped to lead the International Association for Cryptologic Research.
- Dave Nevin: MA in English; Director of the Oregon Research & Teaching Security Operations Center and adjunct to the School of Electrical Engineering and Computer Science; has 20+ years in systems security, architecture and administration; Certified Information Systems Security Professional; experience developing and implementing security policies; experience with training information technology staff in security practices; familiar with numerous laws, standards, policies and regulations bearing on security including EU-GDPR, FERPA, CUI/ NIST SP800-171, PCI-DSS, and Export Control.

- Jesse Walker: PhD in Mathematics; Research Professor and adjunct to the School of Electrical Engineering and Computer Science; previously was Intel's Chief Cryptographer; has collaborated on research and development of security-related aspects of system design for approximately two decades; achieved international impact for discovering a key weakness in what was the most widely-used wireless protocol (WEP), as well as for helping to invent replacement protocols (WPA and WPA2) now in widespread use.
- Kevin McGrath: MS in Computer Science; Senior Instructor in the School of Electrical Engineering and Computer Science; also Security Researcher at McAfee Advanced Threat Research Lab; has taught and researched operating system design and security, as well as other computer science topics, at OSU for 7 years.

j. Faculty resources – full-time, part-time, adjunct.

The first three faculty above are full-time (but will work part-time on leading the proposed certificate program), while the others are part-time.

k. Other staff.

The proposed undergraduate certificate program will be supported by existing staff in the School of Electrical Engineering and Computer Science and in Ecampus. These include:

- The Associate School Head for Online Programs (Section 1.i) will inform and oversee creation of courses for the hybrid and online modalities, as well as lead the evaluation of the program and its teachers.
- The Admissions Coordinator will review student applications per the criteria above (Section 1.e)
- Academic Advisers, including 3-4 in the School plus 4 in Ecampus, together will serve the existing student population both on-campus and online to promote student success (Section 1.e).
- At least one 0.49 FTE graduate Teaching Assistant per course, and/or additional "pool" TAs dedicated to serving Ecampus and hybrid students across all courses in the Portland area, will hold weekend office hours downtown.

l. Facilities, library, and other resources.

The current facilities, library and other resources will adequately support the proposed certificate program.

m. Anticipated start date.

Summer Term 2019 (Banner: 202000)

2. Relationship to Mission and Goals

a. Manner in which the proposed program supports the institution's mission and goals for access; student learning; research, and/or scholarly work; and service.

Security flaws can harm individual consumers worldwide, as well as Oregon companies and others that sell or service affected software. Mistakes that affect military systems, electricity infrastructure, and other mission-critical systems can even threaten the national security of the United States. Therefore, offering a new undergraduate certificate program in the high-impact area of cybersecurity will align with the University's commitment to promote the well-being of Oregon, the nation, and the world. Moreover, the proposed certificate will support the University's education mission by preparing students for obtaining jobs in cybersecurity-related careers.

b. Connection of the proposed program to the institution's strategic priorities and signature areas of focus.

Establishing a technically proficient workforce is essential to Oregon's economic development, and it ties directly to the Healthy Economy strategic priority of OSU.

c. Manner in which the proposed program contributes to Oregon University System goals for access; quality learning; knowledge creation and innovation; and economic and cultural support of Oregon and its communities.

Section 1.e discusses in detail how different aspects of the proposed program will contribute to quality learning, access, and diversity. Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

d. Manner in which the program meets broad statewide needs and enhances the state's capacity to respond effectively to social, economic, and environmental challenges and opportunities.

Sections 1.b, Section 2.a, and 4.a summarize the importance of cybersecurity from an economic standpoint.

3. Accreditation

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

There is no internationally-adopted standard for cybersecurity education, although several companies and societies offer certifications of their own for different subsets of cybersecurity. The closest standard that spans all potential students' interest areas is from NIST's National Initiative for Cybersecurity Education (NICE). Specifically, the NICE Cybersecurity Workforce Framework[20] characterizes the ways in which different cybersecurity professions are similar or different in terms of the capabilities required of professionals.

This framework was used, in combination with a review of the diverse career directions that students are anticipated to take, to identify core technical knowledge and skills essential to a range of different career paths. These core capabilities were then incorporated as learning outcomes into the five required courses of the proposed certificate program. Finally, the proposed certificate program was designed to require students to pursue additional electives in an area relevant to their respective long-term career interests.

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.

Not applicable

[20] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

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.

Not applicable, as there is no applicable accreditation standard.

4. Need

a. Evidence of market demand.

As described in Section 1.a, millions of high-paying jobs in cybersecurity are going unfilled. Relevant statistics include:

- 2.9 million unfilled positions estimated in 2018[21]
- 3.5 million unfilled positions projected in 2021[22]
- Growth rate forecast at 37% from 2012-2022[23]
- Average salary $116k in 2017[24]
- Entry level salary $66k in 2018[25]
- Steep payscale, rising to $233k for chief information security officers in 2018[26]

The underlying source of market demand for cybersecurity professionals is the burgeoning number of massive, expensive security flaws. Relevant statistics include:

- 5,000 publicly revealed breaches in 2017[27]
- 189,445 total known security vulnerabilities in commercial software since 2011, including 17,091 in 2018[28]
- Over 19 billion records affected in total from known breaches between 2015-2018[29]
- Average cost of $7.3M per security breach in the United States in 2017[30]
- $4.7B projected revenue for digital forensics firms (alone) in 2020[31]

As long as the pace and impact of security breaches continues to accelerate, market demand for cybersecurity professionals will likely remain strong, as well.

---

[21] https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/
[22] https://cybersecurityventures.com/jobs/
[23] https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs
[24] https://www.cio.com/article/2383451/
[25] https://tinyurl.com/payscale-entry-level-cyber-sec
[26] https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000
[27] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[28] https://vulndb.cyberriskanalytics.com/
[29] https://www.riskbasedsecurity.com/2018/01/2017-was-a-nightmare-year-for-security/
[30] https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html
[31] https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html

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

Not applicable

c. Manner in which the program would serve the need for improved educational attainment in the region and state.

It is anticipated that the proposed certificate program will help students to advance in their current job or to obtain a more preferred position where they can use their new skills.

d. Manner in which the program would address the civic and cultural demands of citizenship.

As noted in Section 1.a, security flaws threaten the well-being of companies, individuals, and the nation. Many student learning outcomes of required courses within the proposed certificate program therefore pertain to civic and cultural life. To illustrate, consider the first two of these required courses:

- CS 370 - Introduction to Security: This course teaches students about typical threats to privacy, security, accountability and similar fundamental attributes demanded of the systems that pervade everyday life. The course thereby enables students to achieve the learning outcome to "Understand the need for cyber security, key notions of security, and well established security principles and security mechanisms/controls."
- CS 373 - Defense against the Dark Arts: This course teaches students in further detail about threats to security in modern society, so that they can "Demonstrate awareness of the current state of malware, adware, and crypto-ware." Furthermore, it teaches techniques to counter these threats. For example, two other learning outcomes are that students can "Implement spam identification tools" and can "Implement solutions to common attack vectors in multiple environments." The course thus teaches students how to protect against the malware that frequently takes over peoples' computers, against the spam that chokes their communications, and against the crypto-ware that encrypts the hard drives of consumers and companies (then demands a ransom).

5. Outcomes and Quality Assessment

a. Expected learning outcomes of the program.

Students completing the proposed certificate program will be able to:

- Describe the common threats to system security and explain their mechanisms of action
- Assess system requirements pertaining to confidentiality, integrity, and availability of data and functionality to users
- Implement secure solutions to common threats by selecting and applying appropriate principles, protocols and techniques
- Evaluate system designs, implementations and protocols to identify and ameliorate weaknesses

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

Every other spring, the Associate School Head for Online and Continuing Education will email students enrolled in the undergraduate certificate program, inviting them to complete a questionnaire about their perception of what they have learned related to the program learning outcomes. This questionnaire will be designed with the input of the courses' instructors so that, for each of the 4 program learning outcomes, the questionnaire specifies specific elements of specific courses with related course-level learning outcomes. The questionnaire will ask students to rate the effectiveness of those course elements in helping students to achieve the corresponding program-level learning outcomes.

Then, learning outcomes will be identified for which relatively few course elements were rated relevant or beneficial. The Associate School Head will then conduct focus groups with the instructors to solicit their perceptions about the strengths and weaknesses of courses relative to learning outcomes, as a means of cross-validating students' perceptions about these course elements. These conversations with instructors will also aim to identify strategies for improving the curriculum during the subsequent year. Finally, in the following year, the next round of questionnaires will make it possible to assess the extent to which these changes improved student learning outcomes.

c. Program performance indicators, including prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate.

The College of Engineering performs a yearly survey of recent BS graduates using a questionnaire similar to that of the National Association of Colleges and Employers (NACE) First-Destination Survey. The College will augment this survey with new questions enabling it to measure the percent of certificate graduates who report obtaining a job that involves designing, implementing, troubleshooting or managing security-related aspects of systems. These questions will already be part of the survey deployed prior to the graduation of the first cohort of students in the proposed certificate program, thereby providing a baseline for comparison when assessing whether the program aids students in obtaining measurably better career outcomes. In addition, these questions will be part of the survey given to all computer science graduates in the future, making it possible to assess whether students graduating with the proposed undergraduate certificate achieve better career outcomes on the target metric than students lacking the certificate.

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

The College of Engineering has established expectations for the nature and level of research and/or scholarly activity of faculty. The School of Electrical Engineering and Computer Science evaluates all tenure/tenure-track faculty on an annual basis to ensure they meet expectations, and the College of Engineering reviews all faculty considered for tenure and promotion. The proposed undergraduate certificate program will not impact any of these expectations for research and/or scholarly work.

6. Program Integration and Collaboration

a. Closely related programs in other OUS universities and Oregon private institutions.

Several Oregon institutions offer somewhat topically-related initiatives.

- Oregon Institute of Technology (OIT) operates a Cyber Defense Center, within which students learning cybersecurity can practice on companies facing security issues. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[32]
- Portland State University (PSU) has hosted GenCyber summer camps for high schoolers. This does not appear to be a full cybersecurity undergraduate program (even a certificate).[33]
- Mt. Hood Community College (MHCC) offers an Associate of Applied Science in Information Systems and Technology Management in Cyber Security and Networking. The program focuses on hardware- and networking-related aspects of security. It is therefore narrower than the proposed certificate program, which will address hardware, network, software, protocol, mathematical and management aspects of system security.[34]

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.

After the proposed undergraduate certificate program has been implemented, collaborating with the programs above could provide avenues for expanding student headcount and program impact. For example, PSU actively recruits other organizations (including universities) to host their summer camps; serving as a PSU GenCyber camp could enable OSU to more effectively reach seniors in high school, as a means of exciting them about applying to OSU to study cybersecurity further.

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

See 6.b above. Creating a cybersecurity certificate will establish credibility as a potential partner to other organizations and open up opportunities for collaboration.

d. Potential impacts on other programs in the areas of budget, enrollment, faculty workload, and facilities use.

None anticipated.

7. Financial Sustainability (attach Budget Outline)

a. Business plan for the program that anticipates and provides for its long-term 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.

Existing School staff supporting ongoing programs will suffice for offering the proposed certificate program. The curriculum will adapt existing courses, and the College has budgeted for this one-time expense. Faculty teaching the proposed undergraduate certificate program through the first year have already been identified. In addition, a standing hiring committee has been established to continually accept and evaluate applications for positions as instructors across all teaching modalities and locations (Corvallis in-person courses, Ecampus fully-online courses, and Portland hybrid courses). No new demands on library resources are anticipated.

[32] https://www.oit.edu/cyber-defense-center
[33] https://www.gen-cyber.com/
[34] https://www.mhcc.edu/CyberSecurityNetworkingCurriculum/

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

None anticipated.

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

To obtain their required 27 credit-hours for the proposed certificate program, students will typically take 7 courses, which approximately equals the number of sections taught by a 1.0 FTE instructor. Because the projected certificate enrollment is expected to be approximately 15 students (7.5 FTE) per year, the College of Engineering therefore targets a 7.5 student:faculty FTE ratio. The impact on class size is not anticipated to be significant, as the College plans to split sections so they rarely grow beyond 50 students each. This cap is consistent with studies indicating such sizes help contain costs relative to smaller courses,[35] with little negative impact on student outcomes relative to smaller courses.[36,37] In fact, one study indicated that students reported having more meaningful peer interaction in sections of 20-40 students than students did in smaller sections.[38]

d. Resources to be devoted to student recruitment.

The College of Engineering has budgeted for a marketing campaign to be conducted in partnership with Ecampus, as a means of highlighting the College's Portland presence and the availability of the proposed undergraduate certificate program.

8. External Review
(if the proposed program is a graduate level program)

Not applicable

[35] Bettinger, E., Doss, C., Loeb, S., Rogers, A., & Taylor, E. (2017). The Effects of Class Size in Online College Courses: Experimental Evidence. *Economics of Education Review*.
[36] Gorman, C., Webb, D., & Gee, K. (2018). Hierarchical Linear Modeling Approach to Measuring the Effects of Class Size and Other Classroom Characteristics on Student Learning in an Active-Learning Based Introductory Physics Course. arXiv preprint arXiv:1809.00218. https://arxiv.org/ftp/arxiv/papers/1809/1809.00218.pdf
[37] Monks, J. & Schmidt, R. (2011). The Impact of Class Size on Outcomes in Higher Education. *The B.E. Journal of Economic Analysis & Policy, 11*(1), doi:10.2202/1935-1682.2803.
[38] Burruss, N., Billings, D., Brownrigg, V., Skiba, D., & Connors, H. (2008). Class Size as Related to the Use of Technology, Educational Practices, and Outcomes in Web-Based Nursing Courses. *Journal of Professional Nursing*. DOI: https://doi.org/10.1016/j.profnurs.2008.06.002

Christopher Scaffidi

From: Chaplen, Frank William Rowley <Frank.Chaplen@oregonstate.edu>
Sent: Tuesday, November 06, 2018 7:21 AM
To: Christopher Scaffidi
Subject: RE: CyberSecurity -- COE curriculum committee review

The proposed degree certificate looks exciting and the proposal looks complete. No specific comments regarding details at this point and I look forward to seeing the submitted document.

Thanks, Frank

-----Original Message-----
From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Monday, November 5, 2018 10:43 AM
To: Chaplen, Frank William Rowley <Frank.Chaplen@oregonstate.edu>
Subject: RE: CyberSecurity -- COE curriculum committee review

Thanks, Frank.

-----Original Message-----
From: Chaplen, Frank William Rowley [mailto:Frank.Chaplen@oregonstate.edu]
Sent: Monday, November 05, 2018 10:45 AM
To: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Subject: RE: CyberSecurity -- COE curriculum committee review

Chris,

I have some time set aside tomorrow to look over the proposal and will get back to you by COB tomorrow.

Best, Frank

-----Original Message-----
From: Christopher Scaffidi <scaffidc@engr.oregonstate.edu>
Sent: Monday, November 5, 2018 10:39 AM
To: Chaplen, Frank William Rowley <Frank.Chaplen@oregonstate.edu>
Subject: RE: CyberSecurity -- COE curriculum committee review

Frank,

The School of EECS now has approved the CyberSecurity CAT I, which means that I could forward it to the College for review today.

Do you have any feedback about the proposal, that I could incorporate prior to sending it up to the College officially? Or would you prefer at this point just to see it when it comes to you and the COE curriculum committee after I send it to the dean's office?

I'm ok with either and would like to know your preference. Thank you in advance for any feedback that you have.

Best regards,

Chris Scaffidi

-----Original Message-----
From: Chaplen, Frank William Rowley [mailto:Frank.Chaplen@oregonstate.edu]
Sent: Thursday, November 01, 2018 5:31 AM
To: scaffidc@engr.orst.edu <scaffidc@engr.oregonstate.edu>
Subject: RE: CyberSecurity -- COE curriculum committee review

Great! Thank you.

Best, Frank

-----Original Message-----
From: scaffidc@engr.orst.edu <scaffidc@engr.orst.edu>
Sent: Wednesday, October 31, 2018 7:09 PM
To: Chaplen, Frank William Rowley <Frank.Chaplen@oregonstate.edu>
Cc: scaffidc@engr.orst.edu <scaffidc@engr.oregonstate.edu>; chaplenf@onid.oregonstate.edu; jensen@engr.orst.edu; Jensen, Carlos <Carlos.Jensen@oregonstate.edu>; Beach, Gary <Gary.Beach@oregonstate.edu>
Subject: RE: CyberSecurity -- COE curriculum committee review

Frank,

Thank you for your willingness to provide feedback.

Gary Beach gave me a pre-review of a draft already, which provided many helpful suggestions that I've incorporated into the version now available to you.

I appreciate any feedback that you can give.

Best regards,
Chris

Quoting "Chaplen, Frank William Rowley" <Frank.Chaplen@oregonstate.edu>:

> Chris,
>
> I am happy to provide preliminary feedback, although this should not
> be taken as full committee review.
>
> In addition, an appropriate step at this point is to loop Gary Beach
> of the Office of APA into the conversation. He is the Senior
> Curriculum Coordinator with a purview over Cat I proposals.
>
> Best, Frank
> _____
> From: scaffidc@engr.orst.edu [scaffidc@engr.orst.edu]
> Sent: Wednesday, October 31, 2018 4:32 PM
> To: chaplenf@onid.oregonstate.edu
> Cc: jensen@engr.orst.edu; Jensen, Carlos

> Subject: CyberSecurity -- COE curriculum committee review
>
> Frank,
>
> I'm an associate professor helping EECS to prepare a CAT I proposal
> for a new undergraduate certificate in cybersecurity. Carlos Jensen
> indicated that I should provide you with a copy of the proposal for
> feedback.
>
> Would you please be willing to review our proposal at the URL below,
> provide suggestions that you might have, and conduct any vote required
> as part of the approval process? I'm unsure exactly what kind of
> approval process is necessary at this point, prior to the submission
> of the CAT I.
>
> https://docs.google.com/document/d/1l6JIajN8XwwrzZE9hkrE4DahIg8f4DF4Tu
> F0mS06250/
>
> Thank you in advance,
> Chris Scaffidi
> Associate Professor
> School of Electrical Engineering and Computer Science
>

OSU Internal Budget Outline Form

Estimated Costs and Sources of Funds for Proposed Program

Total new resources allocated to the Proposed Program, if any.
If no change in resources is required, the budgetary impact should be reported as zero.

PROGRAM TITLE: Undergraduate Certificate in Cybersecurity

BUDGET PERIOD: From FY 2018-19 to FY 2021-22

Business Center: BEBC Date:
Name and Title of Reviewer:

	One-Time			
	Fiscal Year 1	Fiscal Year 2	Fiscal Year 3	Fiscal Year 4
Personnel				
Faculty, Tenured/Tenure-track	75,000			
Faculty, fixed-term				
Sub-total, Faculty	75,000	-	-	-
Graduate Assistants				
Support Staff				
Fellowship/Scholarship				
OPE	37,500			
Personnel Subtotal	112,500	-	-	-
Other Expenses				
Library, Printed				
Library, Electronic				
Services & Supplies	5,000			
Capital Equipment				
Other Resources Subtotal	5,000	-	-	-
Physical Facilities				
Construction				
Major Renovation				
Other Expenses				
Physical Facilities Subtotal	-	-	-	-
Total Cost of Program	**117,500**	**-**	**-**	**-**
Resources				
Current Budget, unit	110,000			
Tuition (e campus, differential)	75,000			
Institutional Reallocation from other budgetary units				
Special State Appropriation				
Federal Funds and other Grants				
Fees/Sales				
Foundation Endowment				
Tuition remission (GA support)				
Other, describe:				
Total Resources	**185,000**	**-**	**-**	**-**

Note: Please include budget narrative describing items listed above.

OSU Internal Budget Outline Form

Estimated Costs and Sources of Funds for Proposed Program

Total new resources allocated to the Proposed Program, if any.
If no change in resources is required, the budgetary impact should be reported as zero.

PROGRAM TITLE: Undergraduate Certificate in Cybersecurity

BUDGET PERIOD: From FY 2018-19 to FY 2021-22

Business Center: BEBC Date:

Name and Title of Reviewer:

	Recurring			
	Fiscal Year 1	Fiscal Year 2	Fiscal Year 3	Fiscal Year 4
Personnel				
Faculty, Tenured/Tenure-track	60,000	61,800	63,654	65,564
Faculty, fixed-term				
Sub-total, Faculty	60,000	61,800	63,654	65,564
Graduate Assistants				
Support Staff	25,000	25,750	26,523	
Fellowship/Scholarship				
OPE	42,500	45,088	46,441	33,765
Personnel Subtotal	127,500	132,638	136,617	99,329
Other Expenses				
Library, Printed				
Library, Electronic				
Services & Supplies	2,500	3,000	3,000	3,000
Capital Equipment				
Other Resources Subtotal	2,500	3,000	3,000	3,000
Physical Facilities				
Construction				
Major Renovation				
Other Expenses				
Physical Facilities Subtotal	-	-	-	-
Total Cost of Program	**130,000**	**135,638**	**139,617**	**102,329**
Resources				
Current Budget, unit				
Tuition (e campus, differential)	113,760	119,760	122,760	125,760
Institutional Reallocation from other budgetary units				
Special State Appropriation				
Federal Funds and other Grants				
Fees/Sales				
Foundation Endowment				
Tuition remission (GA support)				
Other, describe:				
eCampus Support for Cert, Coord.	25,000	25,000	25,000	
eCampus Travel Support	10,000			
Total Resources	**148,760**	**144,760**	**147,760**	**125,760**

Note: Please include budget narrative describing items listed above.

OSU Internal Budget Outline Form

Estimated Costs and Sources of Funds for Proposed Program

Total new resources allocated to the Proposed Program, if any.
If no change in resources is required, the budgetary impact should be reported as zero.

PROGRAM TITLE: Undergraduate Certificate in Cybersecurity

BUDGET PERIOD: From FY 2018-19 to FY 2021-22

Business Center BEBC Date
Name and Title of Reviewer Signature of Reviewer

	Total			
	Fiscal Year 1	Fiscal Year 2	Fiscal Year 3	Fiscal Year 4
Personnel				
Faculty, Tenured/Tenure-track	135,000	61,800	63,654	65,564
Faculty, fixed-term	-	-	-	-
Sub-total, Faculty	135,000	61,800	63,654	65,564
Graduate Assistants	-	-	-	-
Support Staff	25,000	25,750	26,523	-
Fellowship/Scholarship	-	-	-	-
OPE	80,000	45,088	46,441	33,765
Personnel Subtotal	240,000	132,638	136,617	99,329
Other Expenses				
Library, Printed	-	-	-	-
Library, Electronic	-	-	-	-
Services & Supplies	7,500	3,000	3,000	3,000
Capital Equipment	-	-	-	-
Other Resources Subtotal	7,500	3,000	3,000	3,000
Physical Facilities	-	-	-	-
Construction	-	-	-	-
Major Renovation	-	-	-	-
Other Expenses	-	-	-	-
Physical Facilities Subtotal	-	-	-	-
Check math	-	-	-	-
Total Cost of Program	247,500	135,638	139,617	102,329
Resources				
Current Budget, unit	110,000	-	-	-
Tuition (e campus, differential)	188,760	119,760	122,760	125,760
Institutional Reallocation from other b	-	-	-	-
Special State Appropriation	-	-	-	-
Federal Funds and other Grants	-	-	-	-
Fees/Sales	-	-	-	-
Foundation Endowment	-	-	-	-
Tuition remission (GA support)	-	-	-	-
Other, describe:	-	-	-	-
eCampus Support	25,000	25,000	25,000	-
eCampus Travel Support	10,000	-	-	-
Total Resources	**333,760**	**144,760**	**147,760**	**125,760**
check math	333,760	144,760	147,760	125,760

Note: Please include budget narrative describing items listed above.