ACADEMIC AFFAIRS

FORM 1: Presentation Checklist

Please review the following list of items that must be considered by new programs or significant changes to current programs or policy. Not every item listed is required for each presentation to Academic Affairs. This list serves as a review of potential questions addressed by the Academic Affairs Committee.

Facilitators of new or changing programs or policy should work closely with the curriculum coordinator, appropriate department chair(s) and instructional dean, or with appropriate administrative leadership to review the following list, prior to the first reading with Academic Affairs.

Please note: If an item listed is not relevant to your specific presentation to Academic Affairs, please mark it as **N/A**. Use the last page for your remarks.

OVERVIEW OF PROGRAM OR POLICY

☐ Give rational for new program or changes in current program or policy, including data to support rationale (attach any necessary documents).

BUDGET

☐ Review key budget items.

- Revenue projections based on student enrollment projections or other sources of income, including tuition and fees.
- Start-up budget requirements including salary, benefits, materials and supplies, equipment, facilities
- Post implementation budget including salary, benefits, materials and supplies, equipment, facilities, etc.

INSTRUCTIONAL REQUIREMENTS

☐ Review requirements.

- Current availability of faculty, administration and/or staff.
- Minimum qualifications for faculty, administration and/or staff.
- Potential impacts to all affected academic and other departments.

OPERATIONAL NEEDS, CURRENT AND FUTURE

☐ Review possible operational needs.

- Existing resources including faculty, administration, staff, equipment.
- Involvement of department with oversight of program or process
- Required administrative support.
- Facility needs, including location, amount of space, construction or remodeling requirements.
- Potential impacts to administrative and student support departments including Enrollment services, Financial Aid, CAP Center, Library, Tutoring and Testing, Information Technology Services and others.

STUDENT IMPACT

☐ Identify student impact

- Identify and quantify potential student impact.
- Minimize negative student impact through teach-outs, grandfather clauses, substitutions or other options.
- Communication planning.

ANTICIPATED IMPLEMENTATION TIMELINE

☐ Anticipated Timeline

- Designate affected department(s) and include names and positions of faculty, administration and staff involved in implementation.
- Identify current process adjustments.
- Change General Procedures Manual as needed.
- Communication planning.

Academic Affairs Presentation Checklist

Name: Ralph Phillips **Date**: 11/14/2017

Department: Computer and Information Systems (CIS)

Please note: If an item listed is not relevant to your specific presentation to Academic Affairs, please mark as **N/A**. Use as many pages as necessary.

OVERVIEW OF PROGRAM OR POLICY

AAS in Cybersecurity

The new CIS AAS in Cybersecurity degree is designed to prepare CIS students for entry into the fast-growing field of Cybersecurity as well as provide a guided pathway to Oregon Institute of Technology's B.S. in Cybersecurity degree. With the two-year degree and industry certifications that can be earned in parallel to many of our courses, students will be well positioned to fill entry-level jobs in the Cybersecurity field.

- Following through with a Bachelors, students may see more job opportunities and salaries in excess of $80,000
    - https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
    - http://www.mass.gov/anf/research-and-tech/cyber-security/cyber-security-employment-statistics.html
- Stopping with the AAS and going to work, students will see job opportunities as a junior analyst with salaries greater than $50,000
    - Portland. BA/BS preferred but not required - $68,000 (https://goo.gl/uFG7BN)
    - Bend. Degree or experience and industry certification - $71,000 (https://goo.gl/zDkUgz)
    - In meeting with other employers in Bend, confirmations that the course mix described below and certifications would support entry-level work in security

BUDGET

- This would be a 96-100 credit AAS program, costing the same as others.
- Although there are no special course fees or equipment, students would will be encouraged to pass 3-5 industry certifications along the way or soon after graduating. These certifications tests range in cost from $100 - $200.
- Lead faculty may seek the use of additional PIP funds to support training for future cybersecurity classes.
- There are no start-up costs.

INSTRUCTIONAL REQUIREMENTS

- Likely that existing faculty and part-time instructors in the CIS department can teach all of the essential classes. Most classes in the program are already offered in CIS as part of existing AAS degrees.
- Possible that we will seek out a part-timer with cybersecurity and education skills.
- Possible that we will seek out a replacement FT faculty with cybersecurity/networking skills when needing to replace retiring FT faculty in the next 2-3 years.
- New instructional hires would need computer networking experience and cybersecurity experience. Instructors may have a Bachelor's degree with appropriate experience.
- It is not likely that other COCC departments will be affected.
- There could be some impact to another CIS program: CIS AAS Networking. Networking and Cybersecurity are tangentially related and likely some students that were thinking of going into Networking might opt for Cybersecurity, and vice versa.

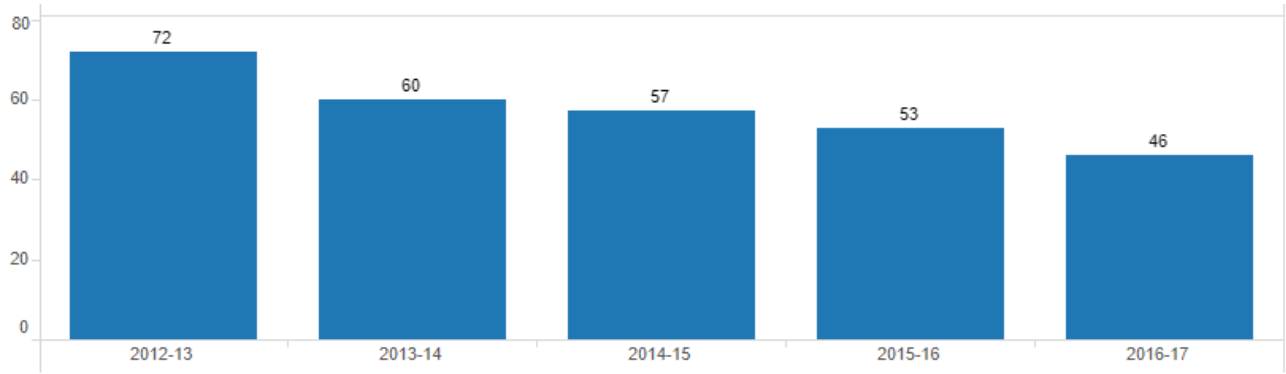
OPERATIONAL NEEDS, CURRENT AND FUTURE

- We expect to utilize existing staff and resources, including a networking lab/classroom in Pioneer Hall 232.
- We do NOT expect any additional impacts on administrative and student support departments.

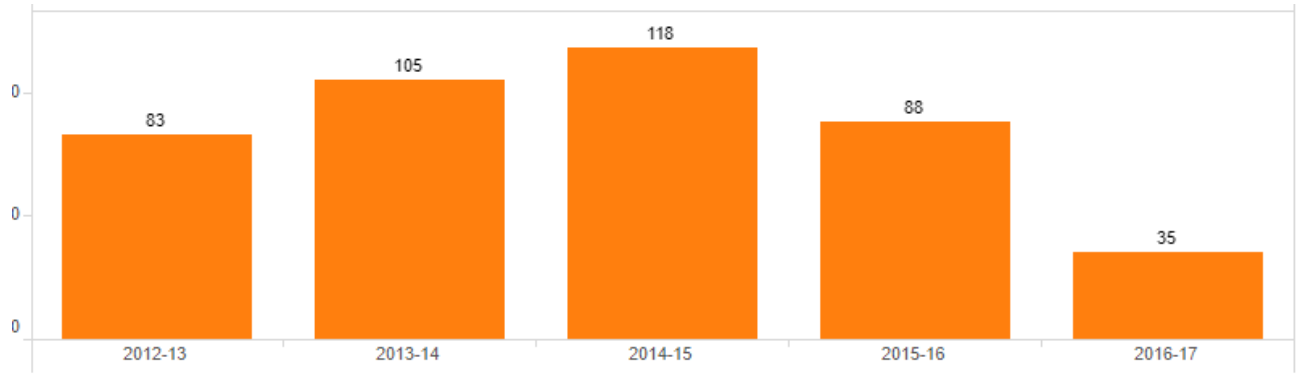
STUDENT IMPACT

- Marketing and education of the program will be critical. The department will work to promote the program to students and solicit help from COCC public relations.
- Students will also need to be prepared for a more challenging entrance into Cybersecurity, compared to a general AAS in Computer and Information Systems. Higher level math and computer understanding for entry-level classes.

Networking Students



Computer Science Students



- Estimating that Cybersecurity students may be 10 the first year, and pick up over several year to similar headcounts with Networking and Computer Science.
- A similar program at Mt Hood Community College saw cybersecurity student enrollment of 42, 66, and 104 in the past three years.

ANTICIPATED IMPLEMENTATION TIMELINE

- We would like this AAS degree listed in the catalog for AY 18-19.
- Students that start the program then will be taking mostly courses that are already available.
- One new 2-credit orientation course will be available in 18-19.
- Other courses would be made available in AY 19-20, if registered students are truly on a 2-year path. Otherwise, those upper-level classes will be available in 20-21.
- Most communication with students in the program will take place with teachers and advisors. It is reasonable that early on, all cybersecurity students will have the same CIS faculty advisor.

EXAMPLE COURSE OFFERINGS LEADING TO AAS CYBERSECURITY

Quarter	Course	Course Title	Credits
	CIS 101 (NEW)	**Cyber Program Orientation *** **	**2**
	CIS 140	A+ Essentials	4
	CIS 145	A+ Essential II	4
	CIS 151 C	Cisco Introduction to Networks	4
	WR 121	English Composition	4
			18
	CIS131 (125E)	Software Applications	4
	CIS 279L	Linux +	4
	CIS 152 C	Cisco Routing and Switching	4
	MTH 95	Intermediate Algebra - MTH 111 Preferred For Transfer	4
			16
	CIS 154 C	Cisco Scaling and Connecting Networks	4
	CIS 279 SE	Security +	4
	SPE 111	Fundamentals of Public Speaking	4
	CIS195	Web Development I	4
	PHL 202	Problems of Philosophy - Ethics	3
			19
	CIS 279 SC	Server Configuration (70-740)	4
	CIS 284	CCNA Security	4
	CIS122 / CS 160	Introduction to Programming	4
	BA 285***	Business Human Relations	3
	PSY 201	Mind and Brain	4
			19
	CIS 279 SM	Server Management (70-741)	4
	CIS284EH	Ethical Hacking	4
	CIS 244	Systems Analysis (Change to Project Manage)	4
	CIS 279 HT (NEW)	**Hacker Tools and Techniques**	**4**
			16
	CIS 279 SS	Server Services (Azure)	
	CIS 279 F (NEW)	**Incident Handling and Forensics**	**4**
	CIS 135 DB /CIS 275	Database	4
	CIS 297 (or CIS 297C)	CIS Capstone (or Cybersecurity Capstone)	3
	or CIS 280	Cooperative Work Experience (Preferred)	
			11
		Total Credits:	**99**

New CTE Program Development Process
Stage 1: Program Abstract Proposal

The "Program Abstract" is the first step for those individuals or teams interested in proposing a new career and technical education (CTE) program. When complete, submit the information to the Vice President for Instruction, who will solicit feedback from the President's Advisory Team and the President. The president may then approve the abstract as is, ask for additional information, or deny the proposal.

Details regarding the full process for developing new CTE programs is available through the Vice President for Instruction's office.

Proposer(s): **CIS Department (Dan Alberghetti, Eric Magidson, Ralph Phillips)**

1. **Program Overview:** Provide a general description of the program and program goals. If the program needs to start quickly, the proposer should indicate whether the program should be offered in a non-credit format and a plan to transition it to credit offerings. If program courses were previously offered as noncredit courses, describe program enrollment trends, program history, and other lessons learned from the noncredit offerings.

   The new CIS AAS in Cybersecurity two-year degree is designed to prepare CIS students for entry into the fast-growing field of Cybersecurity as well as provide a guided pathway to Oregon Institute of Technology's B.S. in Cybersecurity degree. With the two-year degree and industry certifications, that can be earned in parallel to many of our courses, students will be well positioned to fill above entry level jobs in the Cybersecurity field.

   ***** Please review Appendix A – for the current DRAFT of courses to be included in the AAS Cybersecurity degree and their potential transferability to OIT's B.S. in Cyber.**

2. **Strategic Alignment:** Describe how the new program fits with the COCC mission, strategic plan, and accreditation core themes.

   As related to the Core Themes, the new Cybersecurity program would support:

   1. Workforce Development
   WD 2. Deliver CTE curricula that meets current industry standards.
   WD.3 Maintain and strengthen student opportunities in CTE programs for students to achieve program completion and employment in their area of study.

   2. Lifelong Learning

LL.1 Broaden lifelong learning opportunities based on assessed industry, community, and campus needs.
LL.3 Expand options for accessibility and instructional delivery in Continuing Education.

As Related to Strategic Plan, the new Cybersecurity program would support:

1. **Our Vision**
   ***Preparing "students for employment"**
   ***Assisting "regional employers"**

2. **Employment Projections:** Provide evidence of employment opportunities after program completion, including anticipated wage upon entry, wage progression potential and a statement of need for the occupation. Possible resources include: Oregon Labor Market Information System (OLMIS); discussion with the regional economist (541.388.6442 or 541.306.1645); and the U.S. Bureau of Labor Statistics. Professional organizations and other data sources may also be used.

   The labor market analysis should include regional and national data on the following questions, noting that both Central Oregon and national trends may be considered:

   a. Why is this program necessary? **It will help to educate students into the fastest growing (demanded) area within Computer Information Systems (CIS) / Information Technology (IT).**
   b. Does the workforce data show that the proposed program is needed? **Yes.**
   c. Can training be provided without creating a new program? **A degree will provide focused completers in this area of CIS.**
   d. What other data resources have been utilized in addition to the Employment Department, e.g., professional organizations, national census, and regional workforce specialists? **Conference calls with local industry professionals, graduation rates from MHCC, see below, and articles citing the growing demand.**
   e. What career pathways, employment opportunities, and further educational opportunities exist for students who complete the program? **We will be working with Oregon Institute of Technology to create a transfer agreement targeting 80+ credits from the proposed AAS in Cybersecurity degree to transfer into their Bachelors of Information Technology degree they will begin to offer Fall of 2018. *This degree may be completed all online.**

1. **Oregon Occupation & Wage Information shows the lowest 10% of starting jobs as paying $24-$35 per hour ($49,920 to $72.800 per year). For Oregon, this job is expected to grow at a "somewhat faster rate than the statewide average growth rate for all occupations through 2024." (Reference Link)**

2. **Bureau of Labor Statistics, Information Security Analyst median pay is $45 per hour ($93,600 per year). Jobs are expected to "grow much faster than average" at**

18% for 2014-2024. (Reference Link)

3. **CSO Online (June 2017): Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. (Reference Link)**

4. **Mount Hood Community College: Data provided by Wayne Machuca, ISTM/CyberSecurity Program Director.**

5.	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
CIS Grads	34	44	49	82	67	69
ISTM/Cyber				42	66	104

We just Compiled these for a grant we are doing" – Wayne Machuca
****CIS will include Game, the legacy degrees: Networking and OS, web master, and IT tech.**
****ISTM will include CyberSecurity and Networking and CS/Database.**

5. **Federal IT Security Leaders Push for More Training to Boost Cybersecurity Response. The Trump administration's executive order on cybersecurity gives agencies enough direction to guide investments in education and training, officials say. (Reference Link)**

*Jobs in Information Security / Cybersecurity are not location specific and thus graduates of our program could "telecommute" and thus work for companies all around the world while continuing to live in and contribute to the Central Oregon community.

4. **Implementation Timeline:** The typical timeline for implementing a new CTE program is included in Appendix A. Describe the anticipated timeline for program implementation, indicating any modifications to the traditional timeline described in Appendix A. Note that the timeline provided is for a traditional start up only; *extraordinary* resources may allow a more rapid implementation timeline and should be explained in the program proposal.

First course(s) for this degree would be available in Fall 2018, with remaining courses offered strategically so that students are able to graduate within a 2-year timeframe.
***Some may choose to lighten a term by taking courses Summer terms.**

5. **Organizational Structure and Implementation Team:** Identify campus faculty and staff who will be involved in implementing this program, including the program developer, the department to which this program will report, and the chair, dean and other implementation team members. Include specific names and at what stage it is anticipated that a content expert may need to be hired.

Lead Faculty: **Eric Magidson (Program Developer) and Dan Alberghetti**
Department: **Computer and Information Systems (CIS)**

Chair: **Ralph Phillips**
Dean: **Michael Fisher**

5. **Specialized Accreditation:** Indicate whether the program requires specialized accreditation and any known accreditation requirements which may impact program delivery, staffing, budget, or other factors.

   Although special accreditation is not required, earning the National Security Administration (NSA)/ Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense Two-Year Education (CAE-2Y) accreditation will provide nationally recognized and marketable support for our program. *Enrollment in the ISTM program at Mount Hood Community College doubled within one year of their accreditation.

   This accreditation will require a great deal of work, program and course specific changes, submitted and approved by the curriculum committee, over the next year to meet the knowledge unit mappings required in every course within the new certification and proposed AAS in Cybersecurity degree.

6. **Diversity:** Explain how this program may help support or foster diversity of our student population, academic programs, values, or other considerations.

   We have begun to work with the Central Oregon STEM coordinator, Whitney Swander, to review opportunities to better market/promote careers in CIS and Cybersecurity to the woman, Hispanics, and Tribal Members, who traditionally are identified as minority demographic groups within this area.

7. **Exceptional Needs:** Describe extraordinary needs anticipated as a result of this program; this includes teaching and/or support staff, facilities, policy changes, accreditation requirements or other considerations.

   Given the relative newness of cybersecurity, as a focus area within CIS, current COCC instructors will need to be greatly supported with continued educational opportunities that will provide the skills and potential industry certification training needed to successfully educate our students pursuing either the cyber security certificate or proposed degree.

Appendix A

COCC - AAS Cyber					Porposed OIT Transfer		
Qtr	Course	Course Title	Credits	Course Change	Course	Course Title	Credits
First Qtr	CYB 101	Cyber Program Orientation *** (NEW)	1		CYB 101	Cybersecurity Program Orientation	1
	CIS 140	A+ Essentials	4				
	CIS 145	A+ Essential II	4		MIS 145	PC Hardware / Software	4
	CIS 151C	Cisco Introduction to Networks	4		MIS 251	Networking I	4
	WR 121	English Composition	4		WRI 121	English Comp	3
			17				
Second Qtr	CIS131	Software Applications	4		MIS 102	Spreadsheet Software Lab	1
	CIS 279L	Linux +	4		MIS 240	Linux	4
	CIS 152 C	Cisco Routing and Switching	4		MIS 252	Networking II	4
	MTH95	Intermediate Algebra - MTH 111 Preferred For Transferr	4		MTH 111	College Algebra (If Taken)	4
			16				
Third Quarter	CIS 154 C	Cisco Scaling and Connecting Networks	4		MIS 253	Networking III	4
	CIS 279 SE	Security +	4	CYB 279 E	CYB 201	Cybersecurity Fundamentals	4
	SPE 111	Fundamentals of Public Speaking	4		SPE 111	Fundamentals of Speech	3
	CIS195	Web Development I	4		MIS 280	Intro to HTML/CSS	4
	PHL202	Problems of Philosphy - Ethics	3		ART, HUM, LIT, PHL,etc	Humanities Elective	3
			19				
Fourth Qtr	CIS 279 SC	Server Configuration (70-740)	4		MIS 273	Windows Server	4
	CIS 284	CCNA Security	4	CYB 284			
	CIS122 / CS 160	Introduction to Programming	4		CST 116	C++ Programming	4
	BA 285***	Business Human Relations	3		ART, HUM, LIT, PHL,etc	Humanities Elective	3
	PSY 201	Mind and Brain	4		PHY 201	Psychology	3
			19				
Fifth Qtr	CIS 279 SM	Server Management (70-741)	4				
	CIS284EH	Ethical Hacking	4	CYB 284 EH	???		
	CIS 244	Systems Analysis (Change to Project Manage)	4		MGT 335	Project Management	3
	CYB 279 HT (NEW)	Hacker Tools and Techniques	4		CYB 301	Hacker Tools and Techniques	4
			16				
Sixth Qtr	CIS 279 SS	Server Services (Azure)	4		???	Cloud Computing	
	CYB 279 F (NEW)	Incident Handling and Forensics	4		CYB 302	Incident Handling and Forensics	4
	CIS 135 DB		4				
	CIS ???	Capstone	4				
			16				
		Total Credits:	103			TOTAL TRANSFER	68