

Graduate Executive Committee May 8, 2020 Minutes

Attendees:

Voting Members: Brian McAllister, Jeff Ferguson, Jeff Spicher, Mandi Elder, Margaret Harris, Jon Caudill, Cathy Simmons, TS Kalkur, Brandon Vogt, Kathrin Spendier, Janel Owens, Kay Yoon, Leilani Feliciano, Jeff Montez de Oca, David Fenell, Linda Button, Sylvia Mendez Non-Voting Members: Kylie Rossman, Kelli Klebe, Wang Chao, Beth Daniels, Edward Chow, Donald Rabern, David Dubois, Mary Rupp, Stephani Hosain, Sarah Elsey, KrisAnn McBroom, Kristina Ewald, Wendi Clouse

- ME Cybersecurity (Jugal Kalita, Computer Science; see proposal) •
 - This will be an online master's degree. The coursework will be the same as the in-person degree currently offered.
 - The GEC voted to recommend approval (16 Yes, 0 No, 1 Abstain) 0
- Applications from former students and when changing programs (see proposal) •
 - o This is coming forward from previous discussions we have had on the topic. It was also brough to Deans and Associate Deans for input. These are the requested changes that came out of those discussions.
 - The GEC voted to recommend approval of the policy changes to applications and fees (17 Yes, 0 No, 0 Abstain)
- Process for determining equivalency of bachelor's degree (see proposal)
 - In the fall there was a vote to change policy to allow departments to admit someone who has a bachelor's degree equivalent to a degree offered by an accredited institution. This is the follow-up procedure for departments to establish that equivalency.
- Probation Spring 2020 •
 - The campus has decided to delay probation for the spring 2020 semester due to the COVID-19 crisis. Students who would have been dismissed this spring will be given an extension and students who would have been placed on probation are being given a warning.

Announcements

•

- Fall 2020 GEC (may be online) • • September 11, October 9, November 13, December 11

 - Spring 2021 GEC Meetings • February 12, March 12, April 9, May 7 (A week early due to commencement)
- We are keeping track of all program and most academic updates on a new web page for graduate students, • Graduate School COVID-19 Updates and Information webpage: https://www.uccs.edu/graduateschool/covid19-updates
 - Contact Sarah Elsey if you have additions or other feedback: <u>selsey@uccs.edu</u>
- Tuition Matching Grants and Out-of-state recruitment scholarship awardees are due May 28 to • graddocs@uccs.edu. Remember you should be informing your awardees of these awards. These may help to recruit or retain students.

We are exploring options for what the new graduate student welcome event will look like this August. If you have thoughts, please let Sarah know. Currently this event is scheduled for Aug. 17th from 5:00-6:00pm in person at Berger Hall but it is unknown if we will be allowed to gather in large groups by this time. Please encourage your new students to sign up (link on the Graduate School website) for the event so we can notify them of changes if/when they occur.

DRAFT

Proposal for Online ME in Cybersecurity

4/29/2020

1. Introduction

The term Cybersecurity¹ refers to the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. Therefore, the term refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access². The terms Computer Security, Cybersecurity and Information Technology Security are often used synonymously. We use the term Cybersecurity in this document.

The field of Cybersecurity is of growing importance due to increasing reliance on interconnected computer systems that integrate most elements of our daily lives and power our societal, commercial and governmental systems. Computer systems also undergird the foundations of our twenty-first century global relations. The all-pervasive connectivity that we rely on and cherish is achieved through widespread use of the Internet and wireless networks such as Bluetooth and Wi-Fi, and due to the unprecedented growth in development and use of smart devices, large and small, that constitute the Internet of Things. Due to its enormous complexity, achieving cybersecurity is one of the major challenges of the contemporary world³.

2. Need for Cybersecurity Specialists

At the current time, cybersecurity specialists are needed in all levels of our society, from national defense to protect military assets and infrastructure, to safeguard the intellectual properties of private companies, universities, and non-profits. There is a great need for individuals not only trained in the current techniques of cybersecurity, but also individuals who are prepared to move the field into the future through research and innovation. As a result, there is considerable demand for educational programs in Cybersecurity at the graduate level.

In particular, cybersecurity specialists are needed to protect against leaks and breaches—large and small. There were reportedly 668 large-scale such leaks and breaches compromising billions of records between January 1 and July 2, 2018 according to the Identity Theft Resource Center report⁴. The number of breaches between January 1 and August 10th of 2019 was 50% higher than that of 2018⁵. According to securitymagazine.com, the five biggest breaches or leaks of 2019 were a social media profile leak with 4 billion records, Orvibo Smart Home data leak with 2

¹ Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). <u>"Towards a More Representative Definition of Cyber</u> <u>Security"</u>. Journal of Digital Forensics, Security and Law. **12** (2)

² paloaltonetworks.com

³ Stevens, Tim. <u>"Global Cybersecurity: New Directions in Theory and Methods"</u>. *Politics and Governance*. **6** (2)

⁴ <u>https://www.idtheftcenter.org/wp-content/uploads/2018/07/DataBreachReport_2018.pdf</u>

⁵ <u>https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/</u>

billion records, TrueDialog database leak with 1 billion records, First American Financial's real estate title insurance leak with 885 million records, and MondoDB email database leak with 808 million records⁶. The average total cost of a data breach was \$3.86 million, and the average breach cost reduction for organizations using security automation was \$1.55 million according to the 2018 Ponemon Report⁷. The global average cost of a data breach for 2019 was \$3.92 million, a 1.5 percent increase from the 2018 study⁸.

The tremendous immediate need for cybersecurity specialists is buttressed by statistics. For example, in *The New York Times* article, "The Mad Dash to Find a Cybersecurity Force," the journalist reports, "A stunning statistic is reverberating in cybersecurity: An estimated 3.5 million cybersecurity jobs will be available but unfilled by 2021."⁹ According to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), from October 2018 through September 2019, there were 270,000 openings for information security analysts, but only 112,000 individuals were employed in the US in such positions – an annual talent shortfall of 158,000 workers in arguably the most important area of cybersecurity. There were 235,000 additional openings requesting cybersecurity-related skills during this period. Employers are struggling to find workers with the skills needed in cybersecurity. As a result, the average cybersecurity opening takes 20% longer to fill than other IT jobs.

A quick search of the premier job search site indeed.com on April 29th, 2020, showed 17,708 jobs in the US in "cybersecurity", 576 in Colorado, 224 of them in Colorado Springs itself; 24,653 jobs in the USA when searched for "information security analyst, 537 in Colorado, and 188 in Colorado Springs. Monster.com, another job search site listed 39,738 jobs in "cybersecurity" in the USA on the same day, 1,113 jobs in Colorado, 364 in Colorado Springs; when searched for "information security", the corresponding numbers are 50,112, 1,200 and 323, respectively.

The statistics presented above, culled from various relevant sources, clearly establish that there is immense need for cybersecurity specialists in the country, the State of Colorado, and the city of Colorado Springs. This is particularly true in Colorado Springs, with a number of military installations, and a constellation of defense contractors, small companies and start-ups, attempting to build a cybersecurity ecosystem.

3. Institutional/Departmental Capacity

This effort at creating an online Masters of Engineering (ME) program in Cybersecurity complements UCCS's growing prominence as well as ambitions in cybersecurity research and education. UCCS has a PhD program in Security, housed in the Computer Science department. This PhD program is one of a very few programs in this area in the nation, and is listed in various websites, and is ranked as the fourth affordable PhD in Homeland Security¹⁰ in the entire country.

⁶ https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

⁷ https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

⁸ <u>https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/</u>

⁹ <u>https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html?searchResultPosition=2</u>

¹⁰ <u>https://www.gradschoolhub.com/affordable/online/doctorate/homeland-security/</u>

There is an on-campus ME program in Cybersecurity offered by the College of Engineering and Applied Science (EAS) at this time; this is offered as a track in the EAS College's ME program. In general, as a campus, UCCS has a history of providing online education, going back more than a decade. In addition, Computer Science faculty have developed 10 Massive Open Online Courses (MOOCs) in the area of cybersecurity and their prior experience will be beneficial in developing this new program. The CS faculty have also developed three relevant certificates in the past few years. One (Cybersecurity) of this is at the undergraduate level and two (Network Systems Security, and Secure Software) are at the graduate level.

Currently, the Department of Computer Science has five tenure-track faculty members, exclusively in the cybersecurity area: Professors Edward Chow, Sang-Yoon Chang, Yanyan Zhuang, Gedare Bloom and Shuai Li. Of these, four have been hired recently with funding from the State of Colorado, to improve UCCS's research reputation in the area of cybersecurity and provide a higher number of cybersecurity educational programs at all levels. The Computer Science Department has successfully concluded the hiring of a Gallogly Chair for Cybersecurity in the Spring of 2020; the hired individual will start in January 2021, a delayed start due to the current public health situation. The Department was conducting a search for another cybersecurity faculty member in the Spring of 2020, but it was suspended due to the coronavirus pandemic; it is quite likely that this search will be continued in Fall 2020. In addition to the faculty members directly related to cybersecurity, the department has six additional faculty members who engage in cybersecurity-related research and teaching, at least part of the time: Professors Terrance Boult, Xiaobo Zhou, Jugal Kalita, Kristen Walcott, Rory Lewis, and Philip Brown. The department has also has good relationships with a few local cybersecurity individuals who are graduates of our Security PhD program and have been teaching classes as adjunct lecturers: Drs. Richard White, Jason Upchurch and Joshua Alcorn. The availability of a pool of tenured, tenuretrack faculty and adjuncts, who are gualified to perform research and teach in the area of cybersecurity, makes UCCS a perfect venue to start an online ME program in Cybersecurity. The department currently has capacity to introduce 3-5 online classes annually in cybersecurity, starting Fall 2020 to initiate a high quality ME Online in Cybersecurity. However, since these classes are going to be exclusively online, and creating high quality online instruction is timeconsuming, the capacity will be strained, especially because the department boasts a strong research record in terms of publications and grant acquisition, and would want to improve research performance further, there will be need for further hiring of tenure-track faculty as the program grows.

The Computer Science Department has programs in cybersecurity at Bachelors, Masters and PhD levels. The BI in Cybersecurity program has about 100 students, and the PhD program in Security is fairly large with 53 students. The Department is starting a BA in Computer Science in the Fall of 2020, with a track in Cybersecurity. The Masters program, as mentioned earlier, is a professional Masters of Engineering program, housed in the Engineering Dean's office. The program used to be called ME in Information Assurance, but the name was changed to ME in Cybersecurity two years ago. The program has been in place for a number of years, but the student population is small, with about a dozen students. This has been due to lack of advertising dollars, and that it was not a priority for the campus, college or the department. This proposal seeks to create an environment whereby enough advertising and other resources will be

provided with a view to attracting a large number of students to the proposed ME Online program.

4. Summary of the Proposed Program

The faculty of the Department of Computer Science in the College of Engineering and Applied Science (EAS) propose to create a fully online Masters of Engineering degree in Cybersecurity by Fall 2020. The online ME program in cybersecurity being proposed will initially be an online version of the on-campus ME program (although with an enhanced menu of classes over time), and will not require Regent action. As a result, the program can be introduced quickly, if resources are made available in an expedited manner. The envisioned program will be of high quality, and will require 30 credits to complete, and all classes will be delivered online. To get started, the program will introduce five 3-credit classes in 2020-21, and five additional classes in 2021-22. The department will develop a standardized way to deliver the classes to ensure delivery consistency, high quality content and pedagogical needs of the targeted students, but at the same time, allow for flexibility that is called for by the nature of the material covered by the individual classes. We also envision introducing 4-6 additional classes in the future, so that the students have electives to choose from. The classes offered will cover fundamentals of cybersecurity, as well as a number of emergent classes in cybersecurity. Unlike the on-campus ME program, there will be no requirement for a project or thesis¹¹, since these require one-onone student supervision, which is difficult in an online instructional environment.

Since the program is at the Masters level, it will not require program-specific accreditation. The Computer Science Department has capacity to initiate the program without hiring new faculty, but requests budget for development of classes at the outset. As the program grows, the department proposes to hire new faculty, lecturers and teaching assistants so that the quality of the program can be maintained and enhanced, and the program size in terms of students can be scaled. The goal is to develop an online Masters program that attracts a large number of tuitionpaying students, leveraging the high quality of faculty who keep up with the latest developments in cybersecurity in terms of research, publications and visibility in the professional community. The program will also be focused on scalability, as envisioned by campus and university leadership. Scalability will be modeled by ensuring that tenure-track faculty with PhD and expertise in certain sub-areas of cybersecurity develop the online classes, with help from instructional designers, and video and content editors as necessary; one section of the classes will be taught by the tenure-track faculty person who developed the class during scheduled terms, but as additional sections are needed, lecturers or adjuncts will be hired to deliver these sections, under the supervision of the tenure-track faculty person so that consistency and highquality can be maintained. For example, if a class needs five sections at a later term after some growth, a tenure-track faculty member will teach one section, and would coordinate the delivery of the other four sections by lecturers.

¹¹ Our current on-site ME in Cybersecurity has a thesis or project requirement. Appropriate approvals from the Dean of the Graduate School will be obtained.

5. Motivation for an Online ME in Cybersecurity

The main motivation of proposing an ME degree in Cybersecurity is to train technically knowledgeable students in this very important and topical area of immense need. The graduates will primarily work in industry in cybersecurity-focused jobs, but will also become leaders and managers in private industry, and government, including various branches and agencies employed in providing defense, and gathering and processing cyber-intelligence for the country. The admitted students will possess a BS in Computer Science or a related field. The focus will be on developing knowledge, skills, and abilities (KSA) pertaining to cybersecurity. The proposed program is online to cater to the needs of busy professionals in Colorado Springs, Colorado and around the country, who want to retool themselves with advanced knowledge and skills to provide security to computing, networking, storage and other related infrastructure. The program will be also open to non-working students.

In January 2019, *TechCrunch*, a technology-oriented news service, argues, "Seasoned cyber pros typically earn \$95,000 a year, often markedly more, and yet job openings can linger almost indefinitely. The ever-leaner cybersecurity workforce makes many companies desperate for help." And because Colorado universities are not meeting this need, companies and partnering community colleges are creating their own cyber bootcamps like *SecureSet Academy* in Denver enroll "non-programmers, train them in key skills and help them land jobs."¹²

In response to the passage of state *Colorado House Bill 15-1274*, the *Colorado Workforce Development Council* also examined and reported on how best to respond to the cybersecurity shortfall. The council argued that we need to enhance existing IT programs, target veterans, and create more opportunities to entice persons into cybersecurity fields. Specifically, it stated:

- "Efforts should be strengthened to expand the cybersecurity expertise of people already in IT roles that prepare people for full-time cybersecurity positions."
- "A significant percentage of cybersecurity professionals got their start in the industry through their military service."
- "Employers, educators, and workforce organizations should work together to provide increased opportunities for students and job seekers to use their initial cybersecurity knowledge and skills in activities such as capture the flag events, hackathons, cybersecurity competitions, meet up events, and volunteer activities."¹³

Our online ME Online in Cybersecurity will train and transition working professionals and others into the cybersecurity field, paying close attention to our large military and veteran population in Colorado Springs.

The ME Online in Cybersecurity will also complement our well-developed Bachelors programs (BI-in Cybersecurity is a program with robust enrollment, BA-CS which will start in Fall 2020 will have a Cybersecurity track, BS-CS is planning a track possibly starting Fall 2021), and the PhD program in Security, rounding up our offerings. The ME Online program will be of high-quality,

 ¹² <u>https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/</u>
 ¹³ <u>https://www.colorado.gov/pacific/sites/default/files/AppendixD_Cyber_and_Business_Operations_Career_Path_ways_HB15-1274.pdf</u>

with a goal of scaling up to 300-500 tuition-paying students over 5-7 years. The proposal for the program is also consistent with the vision for online education espoused by the Chancellor of UCCS, and the President of the University of Colorado System. It will ensure leadership of UCCS and the University of Colorado in this space for the near- and long-term future.

6. Existing Masters in Cybersecurity Degrees in Colorado

In Colorado, five institutions offer Masters degrees in Cybersecurity or fields related to Cybersecurity. These are listed below.

- 1. Colorado Technical University (CTU) in Colorado Springs offers an MS in Computer Science with a concentration in Cybersecurity Engineering, and another MS In Information Technology with a concentration in Security Management
- 2. Regis University in Denver offers an MS in Information and Cybersecurity degree
- 3. University of Colorado, Boulder offers an MS in Telecommunication with Network Security as emphasis
- 4. University of Denver offers a Master of Engineering in Cybersecurity
- 5. University of Colorado, Colorado Springs offers a Master of Engineering in Cybersecurity

Colorado Technical University and Regis are private, professional schools; Regis and University of Denver are private schools, with high tuition. University of Colorado-Boulder's degree is in a related field, not quite Cybersecurity. University of Colorado-Boulder will be offering a Master of Science in Technology, Cybersecurity and Policy degree Spring 2021, related to what we propose here, but exactly the same since our program is purely technical and Boulder's in not. The proposed online ME program in Cybersecurity at UCCS will build off of, complement and work alongside the on-campus ME program in Cybersecurity at UCCS.

UCCS already has an on-campus ME in Cybersecurity, as indicated above. The proposed online program will be encapsulated within this ME program. The online program will not have any thesis, project or portfolio requirement like the on-campus ME program. Transfers between the two programs may be allowed, up to halfway through the program, not beyond this point.

7. Curriculum

The proposed online ME in Cybersecurity curriculum can potentially be completed online in 2 years, over 4 semesters. We envision the classes being offered over a semester, but it is possible to expedite the delivery of classes to a shorter span, say 8 weeks, as envisioned by the Universiity of Colorado President. The total number of credits required is 30 credits, just like an on-campus Masters program. There is no project or thesis option, since the faculty have decided that these will be difficult to administer on an online format; not only faculty-student interactions and mentoring will be difficult, but also assessing project and theses work against issues such as collaboration with unauthorized individuals and plagiarism will be fraught with difficulty. Up to 6 credits may be transferred from another institution as long as the syllabi are similar and the grade was B or above, based on the approval of the Program Director or the Chair of the Department of Computer Science. The proposed curriculum is given below.

- 3 credits of Policy required:
 - CYS 5950: Homeland Security and Cybersecurity (3 credits)
- 27 credits of Computer Science listed below.
 - Required classes
 - CYS 5200: Computer Architecture (3 credits)
 - CYS 5220: Computer Communication (3 credits)
 - CYS 5910: Fundamentals of Computer/Network Security (3 credits)
 - CYS 5920: Applied Cryptography for Secure Communication (3 credits)
 - Choose 5 from the following 10 classes, as offered online: We will introduce one course in Year 1, and the four additional classes in Year 2 so that there are ten classes available for a student to graduate by the second year. We will introduce additional classes in Years 4 and 5, to provide for a variety of classes from which the students can choose. This will keep the curriculum fresh and up-to-date as well as provide opportunities for new tenure-track faculty members to develop classes suited to their expertise and interest.
 - CYS 5310: Software Requirements and Specifications (3 credits)
 - CYS 5540: Operating Systems Support and Security (3 credits)
 - CYS 5980: System Security (3 credits)
 - CYS 6910: Advanced Systems Security Design (3 credits)
 - CYS 5930: Privacy and Censorship (3 credits)
 - CYS 5990: Anonymous Networks (3 credits)
 - CYS 5860: Machine Learning for Cybersecurity (3 credits)
 - CYS 5940: Ethical Hacking (3 credits)
 - CYS 5960: Wireless and Embedded Systems Security (3 credits)
 - CYS 5970: Software Security (3 credits)

Most of these are adaptations of our current class offerings, and they will be adapted for professional delivery for an online program. A "standard" for delivery format will be developed by the faculty as soon as the ME Online program is approved. Inspirations for standardization will be partially derived from Coursera classes offered by a number of our faculty over the years; these Coursera classes have attracted tens of thousands of students, although not all tuition-paying. Brand new classes include CYS 5540: Operating Systems Support and Security, CYS 5860: Machine Learning for Cybersecurity. New classes may be developed as new tenure-track faculty are hired to teach in the ME Online program. We anticipate a total of 15 different classes taught in the program by the end of five years, so that the students have options; and there is the possibility of developing tracks like the newly started online Masters program in Cybersecurity at Georgia Institute of Technology. Since the proposed program is at Masters level, the instructors teaching the classes will be all at the PhD level, as required by the Higher Learning Commission, the accrediting body for UCCS.

Students who take CYS 5220, CYS 5910, CYS 5920, and CYS 6910 will be able to get Network Systems Security Certificate as they progress through their ME Online program, giving them an early opportunity for documented professional development. This will be similar to on-campus students. This certificate program will also have to be approved by the Graduate Executive Committee.

8. Admission and Other Requirements

Any professionals in the workforce with a Bachelors degree in Computer Science, Software Engineering, Computer Engineering, or a related field like Electrical Engineering or Mathematics who can demonstrate needed math and programming skills will be considered as appropriate for admission. A minimum GPA of 2.7 from an accredited institution will be required. GRE and TOEFL scores may be required for students from abroad. Non-working students with the required academic background will be also be encouraged to apply.

Admissions and graduation requirements will be set by the department. Applications for admission will be reviewed and recommended by the department faculty, although administrative help will be necessary for efficiency in the process. Students will be advised by faculty, as necessary, in addition to staff-level advising. Rules and policies for admission, graduation and other aspects of graduate student progress, will be based on those of UCCS Graduate School.

9. Timeline for Implementation

Below we provide a timeline with milestones to be achieved. We also provide a table indicating planned class offerings, with new launches shown in italics, although adjustments may be made on faculty availability and teaching capacity. To begin with, it will be possible to graduate in two years for students who take classes regularly according to the suggested schedule of classes. Depending on enrollment, classes may be offered more frequently, and graduating in three semesters may become possible.

- 11/2019 Initial curriculum proposal for Masters of Engineering in Cybersecurity
- 5/2020 Training and Workshops for course development
- 6/2020 Start course development
- 8/2020 Launch first three courses.
- 1/2021 Launch next two courses
- 8/2021 Launch next two courses.
- 1/2022 Launch next three courses.

F20	S21	F21	S22	F22	S23	F23	S24	Steady State
CYS 5200	CYS 5310							
CYS 5220	CYS 5910	CYS 5220	CYS 5910	CYS 5220	CYS 5540	CYS 5220	CYS 5540	
CYS 5950		CYS 5950	CYS 5540	CYS 5920	CYS 5910	CYS 5860	CYS 5910	
		CYS 5920	CYS 5980	CYS 5930	CYS 5980	CYS 5920	CYS 5980	
		CYS 5930	CYS 6910	CYS 5950	CYS 6910	CYS 5930	CYS 5990	

				CYS 5860	CYS 5990	CYS 5950	CYS 6910	
						CYS 5960	CYS 5940	
3	2	3	2	6	6	7	7	
			First		Grad		Grad	
			Grad					

5/2022 1st graduate

AY 22/23: Launch two new courses. AY 23/24: Launch two new courses. AY 25/26: Launch two new courses.

10. Workforce Needs

We envision the following personnel needs as we start the online Cybersecurity ME program and as it takes off. We divide the teaching workforce need into three groups: faculty, graduate teaching assistants (GTA), and lecturers. We divide the faculty time into two parts as well: course development time, and course delivery/teaching time. We also need technical and administrative help, as the program grows in size.

Summer 2020 (Pre-launch, Year 0)

- Course Development: We request a bonus stipend of \$10K each for developing a class by a faculty member. This estimate has been derived by the anecdotal evidence that when developing Coursera courses, a single class took up to 300 hours of faculty time. Current faculty will develop the classes. These classes will be taught in Fall 2020 or Spring 2021. We also request GTA summer support for 2 graduate assistants to help with course development and technical preparation to deliver the courses.
- *Equipment*: \$5,000 for cameras, editors, computers, etc., needed to develop course content.

2020-21 and beyond

Five classes will be introduced in Year 1 and five more classes will be introduced in Year 2. We seek development costs for five classes in Summer 2020; these classes will be taught Year 1. We seek development costs for Year 2 classes in Summer 2021. This is because we do not want to jeopardize faculty capacity for research during the academic year. Faculty in Computer Science are quite successful in seeking and receiving research grants, and hence, we do not want to appropriate too much time toward class development by such faculty; as a result, it will be necessary to hire tenure-track faculty and lecturers to maintain requisite teaching capacity as the program grows. Each class taught by full-time faculty will be taught on-load and online. Initially,

we envision the classes to be offered once every two years, although the frequency will be increased as the number of students increases.

• *Tenure-track Faculty*. Since the classes are at Masters level, we want the instructors to be full-time Tenure Track Faculty (TTF) with PhD so that our classes are of the highest quality. Hiring TTFs, who engage in high-quality research, will enhance the reputation of UCCS in cybersecurity, which in turn is likely to attract more students to our program.

The stable state requires 15 classes led by professors with PhD, which means the program will need 5 TTF to cover the program after startup. We will hire a TTF when the number of students hits 60, and thereafter for each increase in the number of student enrollment by an additional 60. This is to ensure that we have enough resources to continue to excel and attract even more students by delivering high-quality education. This assumes that the department will be re-authorized to hire a TTF in cybersecurity that was halted in Spring 2020 due to the coronavirus pandemic.

- Professors (TTF) will be paid \$2,000 as bonus to teach a class for the first time. This is to
 ensure that the classes are offered professionally, and any glitches in first-time offerings
 are quickly rectified. The competition for tuition-paying professional students is intense
 and the students are demanding, and we want to ensure the highest level of delivery and
 content, especially during the beginning of the program and/or when a class is offered
 the first time. Otherwise, bad initial reputation is likely to harm the growth of the
 program.
- Classes will be revised/enhanced every three years. We budget \$3,000 stipend for each course revision and include five revisions each year starting in year 3. This will ensure that the classes are up-to-date in a fast changing field.
- Director/Chair of the Program: There will be considerable amount of work to get the program off the ground. The director/chair will be responsible for assignment of courses to faculty and lecturers; working with faculty in course development; working on curriculum development and modifications; hiring and supervision of GTAs and lecturers; working on admissions and recruitment; supervising administrative help, etc. We expect this will initially be the responsibility of the CS department chair. For this work, a stipend of \$2K is allocated in Year 0; \$5K is allocated in Year 1, then \$15K starting from Year 2 onward, with 3% increases for inflation.
- Graduate Teaching Assistant: Ideally, we need one GTA per course to help answer student questions, hold tutorial sessions, provide supplementary instructions, answer student emails, and anything else that is needed to ensure success and retention of enrolled students. However, we build slowly for 10 GTAs over 5 years to cover 10 classes. We still need additional GTAs to cover the extra elective/optional classes. For each GTA, we cover in-state tuition.

- *Graders:* We need graders for classes. We have assumed that sections will be limited to 25 students. We will have 1 grader hour per 5 students in a class, thus 5 grader hours per section. This is commensurate with grader hours we provide for on-campus classes.
- *Technician:* A full-time technician is included starting Year 2 with 100% FTE allocated to supporting this program. This will enable the professors and teaching assistants who have technical problems to solve them easily, without running to campus IT all the time.
- Administrative Assistant: A full-time administrative assistant included starting Year 4 with 100% FTE allocated to supporting this program. An experienced administrative assistant in the Dean's office, who works with other ME and online programs in the EAS College, will be re-assigned to work on this program to begin with; but as the program grows, there will be need for additional administrative help.
- Lecturers: We will hire lecturers to teach extra sections of classes as the program grows. The scaling model is described in the next section, "Enrollment Projection and Scaling Model."
- No new faculty hire initially: We plan to start offering the necessary classes online in Year 1 without hiring any new faculty member, with the proviso that we will hire as we meet targets we set here. This provision also assumes that the cybersecurity TTF hire that was halted in the Spring of 2020 will be allowed to proceed in Fall 2020-Spring 2021. This is to ensure that classes as outlined here can be offered without compromising faculty research publication and grant-writing capacities, the cornerstones of our reputation in cybersecurity.

11. Enrollment Projection and Scaling Model

The table below shows the expected number of students in the program in the first 5 years (see proforma attached). It is based on realistic or best guess assumptions. This assumes that there is demand locally in Colorado, as well as nationwide. University of Colorado, and UCCS have good reputation in cybersecurity, and with good marketing such projections are attainable. We do not assume any foreign students in this projection because of high American tuition that most foreign students cannot afford. The student enrollment projection assumes the number of out-of-state students to be slightly higher than Colorado resident students.

Year	Number	Faculty Hire						
	Colorado		Out-of-state Non-resident		Non-resident		Total	
	New	Contin	New	Contin	New	Conti n		New TTF hire was scheduled for Spring 2020, but postponed
1	10	0	10	0	0	0	20	

2	25	8	20	8	0	0	61	
3	40	19	40	16	0	0	114	2 TTF
4	55	26	60	32	0	0	179	1 TTF
5	75	36	80	48	0	0	236	1 TTF

As the number of students enrolled in the program grows, we envision teaching multiple sections of classes per year. The professor (TTF) who develops a class will primarily be responsible for the class in terms of curriculum, instructional design, pedagogical considerations and delivery in terms of video development. When multiple sections are needed, we will hire lecturers to teach the additional sections. The lecturers will be paid a stipend to teach a class. The professor who developed the class to begin with will be responsible for supervising the lecturers, help them with course delivery, and coordinate that multiple sections are taught consistently. For this purpose, the original professor will be paid \$1,000 for each section taught using his/her videos and course content.

12. Funding Model

The funding model is given in the attached Excel proforma sheets. Income will be from student tuition. The goal is to provide "world-class courses" as envisioned by President of the University of Colorado, Mark Kennedy, and at the same time grow the cybersecurity capacity for UCCS Computer Science department in terms of tenure-track faculty, graduate students, research, teaching and administration, leading to recursive growth in reputation and also student enrollment in the proposed program.

Wages and Salaries

Tenure-Track Faculty: This program is led by TTF with 2 new hires in Year 3, and 1 new hire in the subsequent two years. The base salaries for these TTF are CS faculty hire salaries proposed in the BA in Computer Science proposal, recently (April 2020) approved by the Regents of the University of Colorado. The discussion on TTF salaries is repeated below.

This special discussion on salaries for incoming TTF is based on comparison with the authoritative survey of US Computer Science faculty salaries performed every year by Computing Research Association (CRA). This survey is called the Taulbee Survey¹⁴ and has been carried out for many years. We include two tables (Table S1 and Table S2) from the Taulbee Survey 2019, reflecting hires in 2018-19, in this report below.

¹⁴ https://cra.org/resources/taulbee-survey/

		Full Pro	ofessor		Associate			Assistant	No	ck	
	In rank 16+ yrs	In rank 8-15 yrs	ln rank 0-7 years	All years in rank	In rank 8+ years	In rank 0-7 years	All years in rank		Teach	Research	Postdoc
N Depts	121	121	123	138	114	126	136	136	104	46	42
N Indiv	730	561	721	2,086	422	569	1,020	1,182	927	275	347
10 %tile	\$134,550	\$130,305	\$125,483	\$129,873	\$99,437	\$105,705	\$102,998	\$93,292	\$63,464	\$62,361	\$44,219
25 %tile	\$148,927	\$147,364	\$139,837	\$145,563	\$106,847	\$113,170	\$110,023	\$98,266	\$73,063	\$66,841	\$49,031
50 %tile	\$172,929	\$167,877	\$153,056	\$164,541	\$114,288	\$123,557	\$119,484	\$105,449	\$83,657	\$90,000	\$56,016
75 %tile	\$199,936	\$195,279	\$176,150	\$186,517	\$128,378	\$133,802	\$132,919	\$114,529	\$96,511	\$122,661	\$66,742
90 %tile	\$223,616	\$214,288	\$194,443	\$198,425	\$140,267	\$144,675	\$145,257	\$122,253	\$117,765	\$153,459	\$72,004

Table SI. Nine-month Salaries, 138 Responses of 195 US CS Departments, Percentiles from Department Averages

Table S2. Nine-month Salaries, 102 Responses of 142 US CS Public (All Public), Percentiles from Department Averages

	Full Professor					Associate		Assistant	No	n-Tenure Tra	ick
	In rank 16+ yrs	In rank 8-15 yrs	In rank 0-7 years	All years in rank	In rank 8+ years	In rank 0-7 years	All years in rank		Teach	Research	Postdoc
N Depts	86	88	91	102	88	91	100	100	79	30	28
N Indiv	512	400	509	1,482	313	381	721	873	671	179	173
10 %tile	\$134,183	\$126,371	\$124,630	\$128,760	\$99,189	\$102,389	\$102,165	\$92,437	\$61,786	\$60,116	\$43,598
25 %tile	\$144,980	\$145,329	\$132,726	\$142,409	\$105,112	\$108,959	\$108,050	\$96,165	\$69,797	\$65,655	\$47,470
50 %tile	\$163,739	\$160,230	\$149,663	\$156,251	\$113,088	\$121,331	\$116,519	\$101,174	\$79,155	\$77,065	\$52,679
75 %tile	\$184,562	\$183,754	\$166,830	\$177,710	\$124,584	\$128,358	\$127,648	\$109,777	\$88,353	\$117,960	\$60,978
90 %tile	\$203,165	\$202,797	\$184,672	\$189,358	\$138,826	\$137,557	\$137,676	\$116,384	\$102,221	\$136,254	\$65,337

Taulbee Table S1 shows salaries of faculty in 138 out of 195 Computer Science departments in the US, and Taulbee Table S2 shows salaries in 102 out of 142 public CS departments. Currently employed assistant professors in the CS department at UCCS are paid at about 10 percentile compared to both tables. These include PhD granting as well as non-PhD granting departments. The Computer Science department at UCCS houses two distinct PhD programs, PhD in Computer Science and PhD in Security, each with about 50-55 students. These represent two of the five PhD programs on campus, excluding professional doctoral programs, and the graduates of these two programs and the funded research supported by these two programs have been instrumental in UCCS obtaining Carnegie R2 status in 2018.

Tenure Track Faculty: To attract and retain high quality faculty¹⁵, we propose that incoming TTF get salary slightly above 25 percentile. If we consider the 25 percentile salary from Taulbee Table S1 for 2018-19, and assume increment of 3% every year, the salary becomes \$110,549 for the first year when we propose to hire a new TTF in this proposal. If we consider the 50 percentile salary from Taulbee Table S1, the salary becomes \$118,630. If we do the same with Taulbee Table S2, the 25 and 50 percentile salaries become \$108,234 and \$113,872 at the time of first TTF hire. To keep things simple, we propose that the assistant professor starting salary in the first year of hire is \$112,000.

¹⁵ The CS department at UCCS lost three pre-tenure, highly successful assistant professors within the past five years, one leaving for Colorado School of Mines, the second to University of Texas at Arlington, and the third to California Polytechnique University in San Luis Obispo. Another faculty member is poised to leave at the end of Spring 2020. A primary reason for leaving has been salary and a secondary reason has been lack of Graduate Teaching Assistants (GTA) at UCCS. In Computer Science and Engineering, GTAs provide for high quality students who help in teaching, but also perform research.

Development Stipends: We budget 5 course development efforts in Summer 2020 (Year 0) to get started quickly. 3 classes will be offered in the fall, and 2 in the spring. We budget for developing the next 5 classes in Year 1. Each class development is given as a \$10K bonus stipend. This amount is commensurate with the expected amount of time needed to develop high-quality online classes.

Class revision/Enhancement: Every three years, classes will be thoroughly revised and enhanced to keep up with the changes in a very dynamic field; otherwise, most courses will become outdated and hence, unattractive to students who expect to be taught the latest advancements as they will enroll in our program to move forward in their careers in cybersecurity. We have budgeted for revision of the courses on a rolling basis starting from Year 3. Each revision is budgeted as a \$3K bonus stipend. Revision is likely to involve discarding some videos, creating new ones, and overhauling every other video in the class.

First-Time Teaching: Teaching will be part of normal full-time faculty workload. Teaching an online course will count the same as a traditional course for faculty members, and all classes taught by full-time faculty will be taught on-load. Each class in the ME Online program will be taught fully online. That said, the first time that a professor teaches a class, there will be a bonus payment of \$3K stipend to ensure that the professor can work out any kinks necessary.

Director of Program/Chair of Department: This position is responsible for program and personnel management, coordinating development of classes, development and update of curriculum on a regular basis, hiring and managing assignment of lecturers and GTAs, student applications and admissions, assessment of classes and learning, handling any complaints and disputes, and any other issues that arise. A payment of \$2K in Year 0, \$5K in the first year, and \$15K in the second year onward, with 3% inflation adjustments, is included for this responsibility.

Supervision of Delivery: As the program grows and class enrollments exceed 25, the faculty that developed a course will supervise the delivery of that content by lecturers and will receive a \$1K bonus stipend for each section of 25 students supervised in this manner. If section sizes exceed 25 students, the stipend will be pro-rated accordingly.

Classified/University Staff

Technicians: In Year 2, we will hire a technician for \$85K whose responsibilities will include providing immediate technical support to the faculty in the development and delivery of online classes, and promptly taking care of any glitches that arise.

Administrative Assistant: In Year 4 we will hire an administrative assistant at \$55K whose responsibilities will include doing paperwork necessary for admission, monitoring student progress, interacting with prospective and enrolled students, interacting with faculty and lecturers, preparing and submitting expense reports, helping in assessment, etc.

Part-time Staff/Other

Lecturers: As the program grows, the scalability model dictates that each class is led by a full-time faculty and additional sections are taught by lecturers. We impose a class section size cap of 25 students; therefore when a class exceeds 25, additional sections will be opened and taught by lecturers. Lecturers are needed to cover the excess sections beginning with 5 in Year 2, and increasing by 10 each year after that based on enrollment projections. Each Lecturer receives \$5K stipend that increases 3% each year for inflation. The lecturer will have to have PhD or must have extensive professional experience in cybersecurity to be able to teach at the Masters level.

Graduate Teaching Assistants Support: Graduate teaching assistants (GTAs) will be hired as discussed above. A GTA costs \$30K in year 1. Costs are increased by 3% every year for inflation.

Graders: Graders are hired as discussed above. Graders are paid \$15 per hour with 3% increase for inflation. There are 5 sections in Year 1, thus 25 grader hours weekly, and we assume 16 weeks for grading, thus the year 1 totals \$15 * 50 * 16 = \$12,000. There are 15 sections in Year 2, thus 75 grader hours, and each additional year adds 10 more sections thus 50 more grader hours.

Operating Expenses

Equipment: To develop the classes, the faculty will need to have access to high quality equipment such as cameras, recording and editing software, etc. We budget \$5K per year for this purpose.

Software Licenses and Computing Services: Some courses use professional software, for example IDA pro assembler/decompiler, or use public cloud-computing services. We budget \$3K per year to support access to the licenses and cloud computing for instructional staff.

Faculty Professional Development: For the faculty to keep up with the growing and changing area of cybersecurity, it will be necessary for the faculty to go to conferences and workshops on a regular basis. Faculty will also need to buy books and other material to keep up-to-date. Furthermore, part-time lecturers will need training and development support. We propose operating expenses to be given to the department for such purposes. We budget \$20-30K for this purpose per year.

Tenure-Track Faculty Startup: To support strong early-career investment in TTF, we include \$75K for each new TTF hire to contribute to the department's startup support of TTF. This support is complementary to other startup received from outside the department.

13. Enrollment Projections and Limitations

If the enrollment is below projection, the resources required, including faculty, lecturers and GTA, will be scaled down proportionally, keeping in mind that enough classes must be taught so that students can graduatee. If the enrollment is above projections, the resources required, including

faculty and GTA, will be scaled up proportionally. If adequate resources are not made available to the department, caps will be placed on the number of admitted students, and the number of sections will be reduced commensurate to the resources available. In the extreme case, lack of resources may force the department and college to wind down the program and close it.

14. Comparison with Existing Programs on Campus

The proposed ME Online program in Cybersecurity is modeled after the ME on-campus degree cybersecurity degree that is currently offered by UCCS. However, here are the major differences.

- The ME Online program has no thesis, project, or portfolio options; it simply requires taking the 10 courses and graduating with a passing GPA average grade of B.
- The ME Online program replace CS5500 Operating System I course with CYS 5540 Operating System Support for Cybersecurity. We have also proposed a few additional classes in the ME Online program to provide a variety of classes to choose from, especially because we envision it will be a fast growing program, with a good marketing budget and full weight of the CU system behind it. Classes taught in this program can then be adapted and taught on-campus as well, if the on-campus program grows.
- The on-campus track student has a choice of working on a Masters thesis or project with a faculty member supervising research and development experiences. The courses taken on-campus can count towards PhD Security written qualifying exam waiver. If an online track student wants to pursue PhD in Security at UCCS, he/she will have to take the PhD Security written qualifying exam, or take a separate test for each class to qualify for the waiver. The on-campus track aims at attracting local professionals and those interested in pursuing PhD degrees and willing to relocate here.
- The online program aims at attracting the worldwide student audience who are interested in pursuing professional careers in cybersecurity, and enroll in a program based on institution reputation, good cybersecurity degree curriculum, and quality graduate courses. One of our goals will be to compete with a reputed institution like Georgia Tech, which has recently developed a Masters program in Cybersecurity with three tracks: Information Security, Energy Systems, and Policy. Each track requires 21 hours of required credits, 6 hours of elective, and 5 hours of practicum.

15. Cybersecurity Faculty

Below, we list the faculty who are currently scheduled to teach classes in the ME Online Program first, followed by other faculty who are involved in cybersecurity research and education as part of their expertise, and then a few others who are graduates of our PhD in Security program and regularly teach

classes in cybersecurity at UCCS. Of the first group, the first five are core cybersecurity faculty, the last two are partially in cybersecurity.

Core Cybersecurity Faculty Teaching Classes in the ME Online Program

- Dr. Edward Chow, Professor: Network security, vulnerability analysis, web app security, critical infrastructure protection
- Dr. Sang-Yoon Chang, Assistant Professor: Network security, wireless communications, and applied cryptography
- Dr. Yanyan Zhuang, Assistant professor: Computer networking, application fault diagnosis, security and privacy, and secure software engineering.
- Dr. Gedare Bloom, Assistant Professor: Computer system security with particular focus on realtime embedded systems.
- Dr. Shuai Li, Assistant Professor: Online privacy and anonymity, designing and measuring privacy enhancing systems.
- Dr. Kristen Justice, Assistant Professor: Software engineering, software testing and debugging in resource-constrained environments, secure software development.
- Dr. Charles Zhou, Professor: Cloud computing, distributed systems, autonomic and sustainable computing, secure cloud computing.
- Dr. Jugal Kalita, Professor: Natural language processing, machine learning, artificial intelligence, machine learning for cybersecurity.

Other Cybersecurity Professors

- Dr. Terrance Boult, Professor: Computer vision, computer security, physical security, machine learning
- Dr. Philip N. Brown, Assistant Professor: Game theory, cyber-physical systems and society-scale economic systems, security as game
- Dr. Shouhui Xu, Gallogly Chair Professor (recently hired in Spring 2020, from University of Texas at San Antonio, to start in January 2021): Cybersecurity, dynamics of cybersecurity, data analytics, security metrics, cryptography systems, and Network Security

Cybersecurity Lecturers

- Dr. Joshua Alcorn, Lecturer: Software-defined networks
- Dr. Richard White, Lecturer: Risk analysis, critical infrastructure protection, homeland security
- Dr. Jason Upchurch, Lecturer: Malware provenance and malware detection

16. Infrastructure

Software infrastructure for course management will be provided by Campus IT.

Cybersecurity Remote Hands-on Lab: Dedicated computing source including high-end Nvidia GPU for password cracking and deep learning based vulnerability analysis, enough computing, storage and networking resources for the virtualized hands-on cybersecurity lab with virtual machines, virtual smartphones, and virtual routers to conduct hands-on security exercises

remotely, will be developed and supported through the instructional technology and other support on campus. These have been budgeted.

17. Marketing:

Marketing will be carried out by campus, in coordination with the system office. \$40K/year has been budgeted for marketing.

Section C: New Applications

Applications for admission to an advanced degree program should be made online through the University of Colorado Colorado Springs Office of Admissions' graduate application. The complete application must include:

- 1. The graduate application
- 2. Official transcripts from degree-granting institutions must be submitted. Additional transcripts may be required to verify prerequisites or major coursework. A final official transcript from degree-granting institution must be verified.
- 3. A nonrefundable application processing fee.
- 4. Test scores, letters of reference, and other materials as required by specific department/program/school/college.
- 5. For international applicants, a score on the Test of English as a Foreign Language (TOEFL), IELTS, or an equivalent if the program/department/school/college agrees to use an alternative proof of language proficiency (e.g., participation in ESL program), and proof of financial support.

See specific program/department/school/college for admission deadlines as well as any other requirements they may have.

A student who wishes to change the major field of study after acceptance in to a program must submit a new graduate application through the online admission application to the new program/department/school/college. follow the practices of the new program they plan to enter into, but the following broad guidelines are expected The new program/department/school/college faculty will evaluate the student for admission. No additional graduate application fee will be required.

- If changing to a program in a different college, the student must submit a new graduate application for the new program and pay the graduate application fee. Dual degree and joint programs may have different processes.
- If changing to a program in a different department within the same college, typically the student must submit a new graduate application for the new program and pay the graduate application fee. However, some colleges may allow an interdepartment transfer without requiring a new application or fee (e.g., when there is one admissions committee for a college).
- If changing programs within the same department, discuss the change with the program director and the program director may submit a change of program to admissions. Departments may have additional internal procedures that may require a new application and fee.

The new program/department/school/college faculty will evaluate the student for admission.

At times, departments/schools/colleges may accept partial applications for a student's regular or provisional admission as long as the applicant submits all material by the deadline date determined by the graduate director.

Section D: Applications by Former Students

A student who was previously admitted to a graduate program, did not complete the degree, is no longer eligible to register at the University, and now wishes to return to school must do the following:

- 1.-_Clarify status with the program to determine eligibility to return and pursue the same degree.
- 2. _After receiving program approval to continue working on the degree, the student must submit a new application to the admissions office before deadlines have passed for the semester of expected return.
- 3. _Student may be held responsible for any curricular changes that have occurred in the program since they were last enrolled.
- 4. A former student will not be charged the graduate school application fee unless any coursework to be applied to the degree was taken more than six years prior to the student's return.<u>4</u>. Any coursework that is more than 6 years old for master's work<u>degrees</u> and 9 years old for PhD work<u>doctorates</u> will need to be validated to be used towards the degree. <u>Departments may have</u> shorter timelines for work needing validation.
- 5. The program may require a new application to be submitted and reviewed for the student to be readmitted to the program. In this situation, a new application fee is required. If the program does not uniformly require a new application, then the program shall contact the <WHO> to reactivate the student.

A student applying to a doctoral program from a master's program in the same department, with no break in attendance, will not be charged should submit an application for the doctoral program and pay the application fee.

A student in a doctoral program who gets a master's degree along the way does not need to submit a new application or pay an application fee

Graduate School Procedures for Determining Degree Equivalency

Hold a baccalaureate degree or a master's degree from an accredited college or university, or demonstrate completion of work equivalent to the baccalaureate or master's degree from an accredited institution

Procedures:

If a program would like to accept a student into a UCCS graduate program who has not received a baccalaureate or master's degree from an accredited college or university, the program needs to provide a justification that the applicant has an academic record that is equivalent to an appropriate degree from an accredited university. The department should submit a letter to the Graduate School with accompanying evidence to justify that previous academic work is equivalent. Typically, the evidence will be academic work. If the program is going to give credit for work experience, the program must follow HLC Accrediting body rules about giving academic credit for work. This may include having published policy and procedure about use of work experience to earn academic credit. The program may use a variety of materials (e.g., transcripts, course descriptions, syllabi) to show equivalency. The program should submit the letter and evidence to the graduate school in an appropriate timeline for review prior to the start of a new term. The Graduate Dean will either agree or disagree with the assessment. If there is agreement, the graduate school will admit the applicant to the degree program. If there is disagreement, the dean may ask for further evidence or will deny the request to the program. The program can appeal the request to the Graduate Executive Committee or a special subcommittee of the Graduate Executive Committee.

Probation

- For spring 2020 semester only, undergraduate and graduate students who fail to meet the conditions of their College's academic probation policy will be granted an automatic abeyance to their suspension and be placed on continued probation for an additional semester. This includes students who do not earn a GPA in the spring 2020 semester as well as students whose spring 2020 GPA does not meet the conditions of their college's probation policy for continued enrollment.
- Additionally, undergraduate and graduate students whose spring 2020 GPA would normally place them on academic probation will instead receive an academic warning and will be given an additional semester to raise their GPA before they are placed on probation at UCCS.
- All other College probation policies remain in effect.